

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 12,184,700 B2
APPLICATION NO. : 17/577237
DATED : December 31, 2024
INVENTOR(S) : Raleigh

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Column 167, Line 11, Claim 1, "a Internet data connection" should be --a secure Internet data connection--.

Column 167, Line 50, Claim 6, "a Internet data connection" should be --a secure Internet data connection--.

Column 168, Line 15, Claim 9, "the Internet data connection" should be --the secure Internet data connection--.

Column 168, Line 27, Claim 9, "a Internet data connection" should be --a secure Internet data connection--.

Signed and Sealed this
Fifteenth Day of April, 2025



Coke Morgan Stewart
Acting Director of the United States Patent and Trademark Office



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850
106963	7590	04/15/2025		
Headwater Research LLC C/O Farjami & Farjami LLP 26522 La Alameda Ave., Suite 360 Mission Viejo, CA 92691			EXAMINER MURILLO GARCIA, FABRICIO R	
			ART UNIT 2633	PAPER NUMBER
			NOTIFICATION DATE 04/15/2025	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@farjami.com
ffarjami@farjami.com
patent@headwaterllc.com

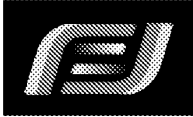
APPLICATION NO.	ISSUE DATE	PATENT NO.
17/577,237	15-Apr-2025	12184700

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

ELECTRONIC CERTIFICATE OF CORRECTION NOTIFICATION

Your electronic certificate of correction is now available, and can be accessed via Patent Center at <https://patentcenter.uspto.gov>.

The electronic certificate of correction is the official certificate of correction under 35 U.S.C. 254 or 255. For more information, please visit <https://www.uspto.gov/electronicgrants>.



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: March 21, 2025

To: Office of Patent Publication, Attention: Certificates of Correction Branch
United States Patent and Trademark Office
Examiner: Murillo Garcia, Fabricio R.; Art Unit: 2633

Re: **Patent No: 12,184,700**
Application Serial No.: 17/577,237
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 4

Message:

Enclosed, please find a Request for a Certificate of Correction due to PTO's Error, and Form PTO-1050.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Raleigh	Group Art Unit: 2633
Patent No.: 12,184,700	Examiner: Murillo Garcia, Fabricio R.
Issue Date: 12/31/2024	
Application Serial No.: 17/577,237	
Filing Date: 1/17/2022	
Title: Automated Device Provisioning and Activation	

REQUEST FOR A CERTIFICATE OF CORRECTION

Commissioner for Patents
Office of Patent Publication
Attention: Certificates of Correction Branch
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

Applicant respectfully requests that a certificate of correction be issued to correct a clerical error introduced due to PTO's error, as shown in the enclosed copy of Form PTO-1050.

The Commissioner is hereby authorized to charge or credit Deposit Account No. **50-0731** for any deficiency or overpayment in the fees required for the filing of this request for a certificate of correction.

Respectfully submitted,
Farjami & Farjami LLP

Dated: March 21, 2025

By: /Farshad Farjami/
Farshad Farjami
Reg. No. 41,014
Attorney for Applicants

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Ste. 360
Mission Viejo, CA 92691
Tel: (949) 282-1000
Fax: (949) 282-1002

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

March 21, 2025
Date

Evan C. Gunderman
Name

/evan c. gunderman/
Signature

**UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION**PATENT NO. : **12,184,700**Page 1 of 1APPLICATION NO. : **17/577,237**ISSUE DATE : **1/17/2022**INVENTOR(S) : **Raleigh**

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the claims, column 167, line 11, "a Internet data connection" should be --a secure Internet data connection--.

In the claims, column 167, line 50, "a Internet data connection" should be --a secure Internet data connection--.

In the claims, column 168, line 15, "the Internet data connection" should be --the secure Internet data connection--.

In the claims, column 168, line 27, "a Internet data connection" should be --a secure Internet data connection--.

MAILING ADDRESS OF SENDER:

PATENT NO: 12,184,700

Farshad Farjani, Esq.
Farjani & Farjani LLP
26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	03/21/2025 05:48:50 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	12184700
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	69691036	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1C1C1_Req_For_Cert_of_Correction_Mar_21_25.pdf	4	-	72 KB
RALEP007C11C3C2C3C2C1C1C1_Req_For_Cert_of_Correction_Mar_21_25-TRAN.LET.pdf	(1-1) 1	Transmittal Letter	31 KB
RALEP007C11C3C2C3C2C1C1C1_Req_For_Cert_of_Correction_Mar_21_25-COCIN.pdf	(2-4) 3	Request for Certificate of Correction	45 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C 1C1_Req_For_Cert_of_Correcti on_Mar_21_25.pdf	21D2024BEA29C6AAF0C41710A5FD1ED63369332ECF7214015 4302044C9F3CC8B8BB3BFA9D1FB6A0853BAAD07AF3A73EF4 60A8576F850B1FC78AE873B1974C4C6
RALEP007C11C3C2C3C2C1C 1C1_Req_For_Cert_of_Correcti on_Mar_21_25-TRAN.LET.pdf	EF9FEDB19C795CB4DF49FB0C7B76C0725BD475FA51ABE310 ECDD0BDAD095A866B21ACDBCCF62C2A00CD4DE9E6F2746 5892AE4C94FF0B5D33112827537C82B04E
RALEP007C11C3C2C3C2C1C 1C1_Req_For_Cert_of_Correcti on_Mar_21_25-COCIN.pdf	2F4EA71E93CEE63B9B3801A99A4766FBDD01DC1BD1A27594 96452FDB8EC2F25A2404A6BFBCA1F6B90C91BAACA2B54F1B E4908A0F5E8CB0721EB3C2D31FC51621

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850
106963	7590	12/31/2024		
Headwater Research LLC C/O Farjami & Farjami LLP 26522 La Alameda Ave., Suite 360 Mission Viejo, CA 92691			EXAMINER MURILLO GARCIA, FABRICIO R	
			ART UNIT 2633	PAPER NUMBER
			NOTIFICATION DATE 12/31/2024	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@farjami.com
ffarjami@farjami.com
patent@headwaterllc.com

APPLICATION NO.	ISSUE DATE	PATENT NO.
17/577,237	31-Dec-2024	12184700

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at <https://patentcenter.uspto.gov>

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit <https://www.uspto.gov/electronicgrants>



FARJAMI & FARJAMI LLP

AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: December 12, 2024

To: United States Patent and Trademark Office
Examiner: Murillo Garcia, Fabricio R.; Art Unit: 2633

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 2,309

Message:

Enclosed, please find:

1. Request for Continued Examination; and
2. Information Disclosure Statement.

Credit card payment in the amount of **\$800.00** as the required Request for Continued Examination fee is hereby included with this filing.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

<h2 style="margin: 0;">REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL</h2> <p style="font-size: small; margin: 10px 0;">Subsection (b) of 35 U.S.C. § 132, effective on May 29, 2000, provides for continued examination of an utility or plant application filed on or after June 8, 1995. See The American Inventors Protection Act of 1999 (AIPA).</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Application Number</td> <td style="padding: 2px;">17/577,237</td> </tr> <tr> <td style="padding: 2px;">Filing Date</td> <td style="padding: 2px;">1/17/2022</td> </tr> <tr> <td style="padding: 2px;">First Named Inventor</td> <td style="padding: 2px;">Raleigh</td> </tr> <tr> <td style="padding: 2px;">Group Art Unit</td> <td style="padding: 2px;">2633</td> </tr> <tr> <td style="padding: 2px;">Examiner Name</td> <td style="padding: 2px;">Murillo Garcia, Fabricio R.</td> </tr> <tr> <td style="padding: 2px;">Attorney Docket Number</td> <td style="padding: 2px;">RALEP007C11C3C2C3C2C1C1 C1</td> </tr> </table>	Application Number	17/577,237	Filing Date	1/17/2022	First Named Inventor	Raleigh	Group Art Unit	2633	Examiner Name	Murillo Garcia, Fabricio R.	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1 C1
Application Number	17/577,237												
Filing Date	1/17/2022												
First Named Inventor	Raleigh												
Group Art Unit	2633												
Examiner Name	Murillo Garcia, Fabricio R.												
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1 C1												

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.

NOTE: 37 C.F.R. § 1.114 is effective on May 29, 2000. If the above-identified application was filed prior to May 29, 2000, applicant may wish to consider filing a continued prosecution application (CPA) under 37 C.F.R. § 1.53 (d) (PTO/SB/29) instead of a RCE to be eligible for the patent term adjustment provisions of the AIPA. See Changes to Application Examination and Provisional Application Practice, Final Rule, 65 Fed. Reg. 50092 (Aug. 16, 2000); Interim Rule, 65 Fed. Reg. 14865 (Mar. 20, 2000), 1233 Off. Gaz. Pat. Office 47 (Apr. 11, 2000), which established RCE practice.

1. **Submission required under 37 C.F.R. § 1.114**
 - a. ☐ Previously submitted
 - i. ☐ Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on _____
(Any unentered amendment(s) referred to above will be entered).
 - ii. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
 - iii. ☐ Other _____
 - b. ☒ Enclosed
 - i. ☐ Amendment/Reply
 - ii. ☐ Affidavit(s)/Declaration(s)
 - iii. ☒ Information Disclosure Statement (IDS)
 - iv. ☐ Other _____
2. **Miscellaneous**
 - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months, Fee under 37 C.F.R. § 1.17(i) required)
 - b. ☐ Other _____
3. **Fees** The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed.
 - a. ☒ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. **50-0731**
 - i. ☒ RCE fee required under 37 C.F.R. § 1.17(e)
 - ii. ☒ Extension of time fee (37 C.F.R. §§ 1.136 and 1.17)
 - iii. ☐ Other _____
 - b. ☐ Check in the amount of \$ _____ enclosed.
 - c. ☒ Payment to be charged by Credit Card in the amount of \$ **800.00**.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print/Type)	Farshad Farjami, Esq.	Registration No. (Attorney/Agent)	41,014
Signature	/Farshad Farjami/	Date	December 12, 2024

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: **Mail Stop RCE**, Commissioner For Patents, P. O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office on:

Name (Print/Type)	Evan C. Gunderman	Date	December 12, 2024
Signature	/evan c. gunderman/		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9,198,117		2015-01-24	Raleigh, et al.	
	2	8,099,764		2012-01-17	Herzog, et al	
	3	8,719,391		2014-05-06	Hämäläinen, et al	
	4	8,041,816		2011-10-18	Ozaki et al	
	5	7,509,487		2009-03-24	Lu	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040122907		2004-06-24	Chou, et al	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2633	
	Examiner Name		Murillo Garcia, Fabricio R.	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	2	20080215883		2008-09-04	Fok, et al	
	3	20060294370		2006-12-28	Greenspan, et al	
	4	20090019517		2009-01-15	Turakhia, et al	
	5	20070011736		2007-01-11	Kalibjian, et al	
	6	20090249084		2009-10-01	Ogawa, et al	
	7	20090286512		2009-11-19	Huber, et al	
	8	20040105431		2004-06-03	Monjas-Llorente, et al	
	9	20070008980		2007-01-11	Dommety et al	
	10	20060239276		2006-10-26	Rodbarry et al	
	11	20090240807		2009-09-24	Munson et al	
	12	20080046727		2008-02-21	Kanekar et al	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	13	20050207379		2005-09-22	Shen	
--	----	-------------	--	------------	------	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2008/048075	WO		2008-04-24	Intro Mobile Co. Ltd.		☐
	2	2006/077283	WO		2006-07-27	Stream Mobile OY		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Excerpts from the Prosecution History of U.S. Patent No. 9,198,117	☐
	2	Declaration and Curriculum Vitae of Dr. Patrick Traynor	☐
	3	3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2	☐
	4	Security Engineering, Second Edition	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	5	Open Mobile Alliance; OMA-WAP-ProvCont-v1_1-20021112-C, Provisioning Content Version 1.1, URL: http://www.openmobilealliance.org/	☐
	6	Open Mobile Alliance; OMA-MMS-ENC-v1_2, Multimedia Messaging Service, Encapsulation Protocol, Version 1.2-20050301 URL: http://www.openmobilealliance.org	☐
	7	Open Mobile Alliance; OMA-ERELED-MMS-v1_2-20030923-C, Enabler Release Definition for MMS Version 1.2, URL: http://www.openmobilealliance.org/	☐
	8	Open Mobile Alliance; Multimedia Messaging Service Architecture Overview (MMSARCH) specification ("OMA") 20030920	☐
	9	Transporting data between wireless applications using a messaging system—MMS (Wireless Comms. and Mobile Computing, July 7, 2006) ("Mostafa")	☐
	10	Declaration of Friedhelm Rodermund	☐
	11	Request for Ex Parte ReExamination of U.S. Patent No. 9,198,117, Application Serial No. 90/019,753, Filed December 3, 2024	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2633
	Examiner Name	Murillo Garcia, Fabricio R.
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-12-12
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

APPENDIX H

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/048075 A1

(51) International Patent Classification:
H04Q 7/24 (2006.01)

(74) Agent: **JIMYUNG Patent Firm**; 6F, Jungwoo Bldg.,
1689-1, Seocho-4-dong, Seocho-gu, Seoul 137-882 (KR).

(21) International Application Number:
PCT/KR2007/005155

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2006-0101714 19 October 2006 (19.10.2006) KR

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant (*for all designated States except US*): **INTRO MOBILE CO., LTD.** [KR/KR]; 2502-Ho, ASEM Tower, 159, Samseong-dong, Gangnam-gu, Seoul 135-798 (KR).

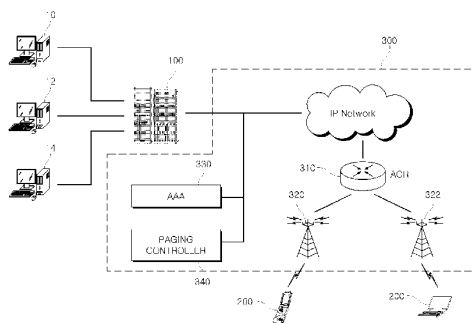
(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **LEE, Changseok** [KR/KR]; LG Apt. 101-1602, 12-2, Gaepo-dong, Gangnam-gu, Seoul 135-939 (KR).

Published:

— with international search report

(54) Title: SYSTEM OF PROVIDING INTEGRATED PUSH SERVICE AND METHOD THEROF



(57) Abstract: The present invention relates to a system and a method for providing an integrated push service in an internet service network, and the integrated push service system comprises a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data; an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push; a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information, wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.

Description

SYSTEM OF PROVIDING INTEGRATED PUSH SERVICE AND METHOD THEROF

Technical Field

- [1] The present invention relates to a system and a method for providing an integrated push service in a network including a mobile internet such as Wibro.

Background Art

- [2] A mobile internet service such as a data service such as WAP (Wireless Application Protocol) based on a mobile communication network such as CDMA2000 1X, 3X, EV-DO, GSM and WCDMA, Wibro (Wireless Broadband) and HPi (High Speed Portable internet) are used to provide a data communication service such as the Internet through a mobile terminal. However, because the mobile communication network is mainly for a voice call and has complex network structure, a cost for building the mobile communication network is high. Therefore, a price per packet is excessive and the mobile communication network is not suitable for the Internet service based on a large capacity multimedia. The mobile internet service is to solve above-described problem wherein a conventional IP network is used to a maximum and a network structure is simple concentrating on a transmission of an IP packet. Therefore, the cost for building the network is low and the price per packet is low. Accordingly, an MBMM (Multiband Multimode) terminal using a conventional CDMA mobile communication modem for the voice call and the mobile internet such as Wibro for a data communication is used.
- [3] On the other hand, a push service is widely used for a sophisticated communication service. The push service actively transmits a data to a client by a server without a user intervention. For instance, an information selected by a user (a news, a stock information and a sports information) is provided to a user terminal in real time or a data for an upgrade is automatically transmitted to the user terminal in order to increase a user convenience.
- [4] However, when the push service is provided via the mobile internet network, problems described below occur.
- [5] First, since a push application server and a push application client should be built for each of the push services, an integrated operation of the network is difficult and a traffic increasing rapidly due to the push service is difficult to manage. In addition, in order to receive the push service in real time, the mobile terminal should load an application or an agent program for each of the push services in a memory. Therefore, a system efficiency is degraded due to a characteristic of the mobile terminal having

limited memory capacity, data processing capacity and battery capacity.

- [6] Second, the mobile terminal enters an idle mode when a data is not transceived considering a mobility of the mobile terminal in case of the mobile internet. In the idle mode, a generation of an unnecessary hand-over traffic is eliminated when moving between base stations in order to minimize a power consumption of the mobile terminal and enable an efficient use of a base station resources. However, in the idle mode, a push data cannot be transmitted to the mobile terminal in real time because the data is not transceived and a connection to a RAS (Radio Access Station) is disengaged.

- [7] Third, since the RAS used in the mobile internet service has a small service coverage compared to a mobile communication base station, a radio frequency shadow area is relatively large and the push data cannot be transmitted in real time when the mobile terminal in the shadow area.

Disclosure of Invention

Technical Problem

- [8] It is an object of the present invention to provide a system and a method for providing an integrated push service wherein various push data generated from a plurality of push application servers are transmitted through an integrated push service server and a mobile terminal extracts an associated application ID app_ID and loads an integrated push service agent selectively invoking a corresponding application to provide the various push services through a mobile internet network, and wherein a separate module for a transmission of the push data is not required for the push service server to reduce a cost for building the push service server, and wherein only a single integrated push service agent is loaded in a memory of the mobile terminal to optimize a system resource of the mobile terminal.
- [9] It is another object of the present invention to provide a system and a method for providing an integrated push service wherein an integrated push service server determines whether a receiving mobile terminal is in an idle mode and a push information is broadcasted via a paging controller provided by a mobile internet service network when the mobile terminal is in the idle mode to provide the push information in real time even to the mobile terminal having a communication session with the integrated push service server terminated in the idle mode.
- [10] It is yet another object of the present invention to provide a system and a method for providing an integrated push service wherein an integrated push service server transmits a push service as an SMS via a mobile communication service network instead of a mobile internet network when a receiving mobile terminal is not connected to the mobile internet network to provide the push information in real time even when

the mobile terminal of a user is in a shadow area of a mobile internet service.

Technical Solution

[11] In order to achieve above-described object, there is provided an integrated push service system comprising: a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data; an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push; a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information, wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.

[12] There is also provided a method for providing an integrated push service comprising steps of: (a) transmitting a push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data and an associated application ID specifying the application for invoking the push data to an integrated push service server through a communication network; (b) transmitting the push information to the receiving mobile terminal via an IP push through a mobile internet service network using the integrated push service server; and (c) receiving the push information using an integrated push service agent resident in a memory of the mobile terminal, and invoking the application compliant to the associated application ID to deliver the push data.

Advantageous Effects

[13] In accordance with the system and the method for providing the integrated push service of the present invention, the various push data generated from the plurality of push application servers are transmitted through the integrated push service server and the mobile terminal extracts the associated application ID app_ID and loads the

integrated push service agent selectively invoking the corresponding application to provide the various push services through the mobile internet network, the separate module for the transmission of the push data is not required for the push service server to reduce the cost for building the push service server, and only the single integrated push service agent is loaded in the memory of the mobile terminal to optimize the system resource of the mobile terminal.

[14] In accordance with the system and the method for providing the integrated push service of the present invention, the integrated push service server determines whether the receiving mobile terminal is in the idle mode and the push information is broadcasted via the paging controller provided by the mobile internet service network when the mobile terminal is in the idle mode to provide the push information in real time even to the mobile terminal having the communication session with the integrated push service server terminated in the idle mode.

[15] In accordance with the system and the method for providing the integrated push service wherein the integrated push service server transmits the push service as the SMS via the mobile communication service network instead of the mobile internet network when the receiving mobile terminal is not connected to the mobile internet network to provide the push information in real time even when the mobile terminal of the user is in the shadow area of the mobile internet service.

Brief Description of the Drawings

[16] Fig. 1 is a diagram illustrating a configuration of an integrated push service system in accordance with an embodiment of the present invention.

[17] Fig. 2 is a diagram illustrating a configuration of an integrated push service server in accordance with an embodiment of the present invention.

[18] Fig. 3 is a diagram illustrating a configuration of an integrated push service agent in accordance with an embodiment of the present invention.

[19] Fig. 4 is a diagram illustrating a hierarchy of an integrated push service agent in accordance with an embodiment of the present invention.

[20] Fig. 5 is a diagram illustrating a configuration of an integrated push service agent in accordance with an embodiment of the present invention.

[21] Figs. 6 through 8 are diagrams illustrating a communication system of a method for providing an integrated push service in accordance with an embodiment of the present invention.

Mode for the Invention

[22] Fig. 1 is a diagram illustrating a configuration of an integrated push service system in accordance with an embodiment of the present invention. Referring to Fig. 1, the integrated push service system comprises a plurality of push application servers 10, 12

and 14, an integrated push service server 100, a mobile internet service network 300, and a mobile terminal 200 including an integrated push service agent 250. The plurality of push application servers 10, 12 and 14 provides a push data to a push service application stored in the mobile terminal 200. The plurality of push application servers 10, 12 and 14 generate the push data push_data such as a real time news data for a news application, a chatting message for a peer-to-peer messenger application and an e-mail message for an e-mail application. A push information push_info including a receiving mobile terminal information specifying the mobile terminal that receives the push data, and an associated application ID app_ID specifying the application for invoking the push data along with the push data is also generated.

[23] In accordance with a conventional push application server, the associated application ID app_ID is not required because the conventional push application server is built for a single push application and a communication session and a protocol are maintained for each of the servers. However, in accordance with the present invention, various push services provided to each of applications are managed in an integrated fashion through the integrated push service server 100 and the integrated push service agent 250. Therefore, the associated application ID app_ID specifying the application for invoking the push data is required.

[24] <Transmission of the push information through an IP push>

[25] The integrated push service server 100 receives the push information push_info from the plurality of push application servers 10, 12 and 14 connected through a communication network, and provides the push information push_info to the mobile terminal 200 through an IP push push_IP. Because the mobile terminal 200 maintains a communication session with the integrated push service server 100 through a CSM (Communication Session Manager) 251 of the integrated push service agent 250, the push information push_info including the push data may be transmitted through the IP push push_IP. When the push information push_info is transmitted through the IP push push_IP, the integrated push service server 100 requests the IP push to the mobile internet service network 300.

[26] The mobile terminal 200 transmits a push information acknowledge message ack_push to the integrated push service server 100 when the push information push_info is received. the integrated push service server 100 acknowledges a successful transmission of the push data by receiving the push information acknowledge message ack_push at a reception acknowledge unit 142. A transmission report manager 140 transmits an information on the reception and a push application service to each of the plurality of push application servers 10, 12 and 14 as a transmission report.

[27] The mobile internet service network 300 is a high speed wireless internet service

such as Wibro and HPI which carries out a communication between the integrated push service server 100 and the mobile terminal 200, transmission/reception of the IP push data push_IP.

[28] The mobile terminal 200 receives the push information push_info in a form of the IP push push_IP through a mobile internet modem 210 for connecting to the mobile internet service network 300, and includes at least one application 260 that is to be associated with the push information push_info. Particularly, the mobile terminal 200 includes the integrated push service agent 250. The integrated push service agent 250 includes the CSM 251 resident on a memory of the mobile terminal 200 that maintains the communication session with the integrated push service server 100 in a state that the mobile internet modem 210 is connected to the mobile internet service network 300, and selectively invokes the application 260 compliant to the associated application ID app_ID of the push information push_info to deliver the push data.

[29] When an entirety of the applications 260 supporting a plurality of push services such as a chatting service, a mail service, a news service and a stock service in the mobile terminal 200 are resident in the memory in order to correspond to individual IP push in accordance with conventional art, a system resources of the mobile terminal 200 may be overloaded to degrade a processing speed thereof and is wasted. However, as shown in Fig. 3, only the integrated push service agent 250 of the mobile terminal 200 is resident in the memory of the mobile terminal 200 with each of the applications 260 being inactive in accordance with the embodiment of the present invention while an IP push receiver 252 receives the push information push_info for the entirety of the applications in an integrated fashion and uses the associated application ID app_ID included in the push information push_info to selectively invoke the application 260 corresponding to the associated application ID app_ID, thereby reducing a number of the applications resident in the memory and a power consumption of the mobile terminal 200.

[30] <Transmission of push information via paging message>

[31] On the other hand, a mobile internet service generally supports a power saving mode in order to reduce power consumption in a mobile environment. The mobile terminal 200 typically updates to which RAS 320 of a plurality of RASs 320 and 322 through a constant communication and a hand-over with the RASs 320 and 322. However, an unnecessary power consumption occurs for the mobile terminal 200 that does not have a constant transmission/reception of a data in order to maintain the constant communication with the mobile internet service network 300 for the hand-over and a registration of the RAS. As a result, the unnecessary power consumption has a serious effect on a DBDM(dual-band dual-mode) terminal using both the mobile internet service network 300 and a mobile communication service network 400 such as

a CDMA and a GSM or MBMM(multi-band multi-mode) terminal supporting three or more communication services.

- [32] The power saving mode provided by the mobile internet service is to solve above-described problem. In the power saving mode, the mobile terminal 200 enters an idle mode wherein a connection to the RAS 320 is lost when an exchange of the data with a mobile internet network is not carried out for more than a predetermined time. The idle mode refers to a state that the transmission/reception of the data by the mobile terminal 200 is not carried out and the connection to the RAS 320 is lost to eliminate a generation of an unnecessary hand-over traffic between the mobile terminal 200 and the RASs 320 and 322, thereby minimizing the power consumption of the mobile terminal 200 and enabling an efficient use of the RASs 320 and 322.
- [33] When a packet to be transmitted to the mobile terminal 200 is generated in the idle mode, a paging controller 340 of the mobile internet service network 300 broadcasts a paging message through the RASs 320 and 322 of a paging group consisting of the plurality of RASs wherein the mobile terminal 200 expected to exist. Through this process, the mobile terminal 200 receives a downlink data packet to exit the idle mode and enter a normal mode to re-connect to the mobile internet service network 300.
- [34] In accordance with the embodiment of the present invention, a push service may be provided continuously for the mobile terminal 200 in the idle mode by transmitting the push information through the paging message. When the mobile terminal 200 enters the idle mode, the CSM 251 of the integrated push service agent 250 of the mobile terminal 200 cannot send the push information push_info through the IP push push_IP because the communication session with the integrated push service server 100 is terminated. While the integrated push service server 100 may schedule and transmit the push information push_info or re-transmit the push information push_info by recognizing a communication configuration of the mobile terminal 200, the push service cannot be provided in real time.
- [35] It is preferable that the push information push_info is included in the paging message instead of the IP push push_IP such that the push service is provided to the mobile terminal 200 in real time in order to solve above-described problem.
- [36] There are two methods for the mobile terminal 200 to recognize the idle mode of the mobile terminal 200. In accordance with a first method, whether the mobile terminal 200 is in the idle mode is registered in a presence server 130 such that the integrated push service server 100 may inquire the presence server 130 of whether the mobile terminal 200 is in the idle mode prior to transmitting the push information push_info. In accordance with a second method, the integrated push service server 100 transmits the push information push_info by the IP push push_IP and determines that the mobile terminal 200 is in the idle mode when the push information acknowledge

message ack_push is not received from the mobile terminal 200.

[37] While a configuration of the integrated push service server 100 is complex due to an association with the presence server 130, an unnecessary IP push is omitted to enable an efficient use of a network resource in accordance with the first method. While an unnecessary traffic is generated due to the IP push push_IP, the integrated push service server 100 does not require the association with the presence server 130, thereby simplifying a system configuration in accordance with the second method.

[38] The first method wherein the presence server 130 is used is described below in detail.

[39] In accordance with first method, the integrated push service server 100 or the mobile internet service network 300 further includes the presence server 130 that determines whether the mobile terminal 200 is in the idle mode, and also further comprises the paging controller 340 for broadcasting the paging message for the mobile terminal 200 through the at least one RASs 320 and 322. The integrated push service server 100 provides the push information push_info to the paging controller 340 when the mobile terminal 200 is determined to be in the idle mode using the presence server 130, and the integrated push service agent further comprises a paging message parser 253 for parsing the push information push_info when the push information push_info is received as the paging message push_paging.

[40] In accordance with first method, the integrated push service server 100 inquires the presence server 130 of whether the mobile terminal 200 is in the idle mode and transmits the push information push_info as the paging message push_paging through the paging controller 340 instead of the IP push push_IP in the idle mode. The mobile terminal 200 extracts the push data push_data and the associated application ID app_ID from the paging message push_paging through the paging message parser 253 as the paging message push_paging is received. The corresponding application 260 is then invoked to provide various push services between the plurality of push application servers 10, 12 and 14 and the mobile terminal 200.

[41] The second method wherein the presence server 130 is not used is described below in detail.

[42] In accordance with second method, the integrated push service agent 250 further comprises a reception acknowledge report manager 256 for generating the push information acknowledge message ack_push, and the mobile internet service network 300 further comprises the paging controller 340 for broadcasting the paging message for the mobile terminal 200 through the at least one RASs 320 and 322. The integrated push service server 100 provides the push information push_info to the paging controller 340 when the push information acknowledge message ack_push is not received from the reception acknowledge report manager 256, and the mobile terminal

200 is configured to further include the paging message parser 253 for parsing for parsing the push information push_info when the push information push_info is received as the paging message push_paging.

[43] In accordance with second method, the integrated push service server 100 transmits the push information push_info via the IP push push_IP and determines that the mobile terminal 200 is in the idle mode when the push information acknowledge message ack_push is not received. The mobile terminal 200 extracts the push data push_data and the associated application ID app_ID from the paging message push_paging through the paging message parser 253 as the paging message push_paging is received. The corresponding application 260 is then invoked to provide various push services between the plurality of push application servers 10, 12 and 14 and the mobile terminal 200.

[44] In accordance with the embodiment wherein the push information push_info is transmitted through the paging message push_paging, it preferable that the CSM 251 of the integrated push service agent 250 of the mobile terminal 200 controls the mobile internet modem 210 to configure the communication session between the integrated push service server 100 and the integrated push service agent 250. In case that the push data push_data is too large to be transmitted efficiently by only the paging message push_paging or that other data is to be transmitted after the transmission of the push information push_info, the mobile terminal 200 automatically exits the idle mode to configure the communication session with the integrated push service server 100 when the push information push_info is received as the paging message push_paging, thereby efficiently providing the push service.

[45] <Transmission of push information through SMS of service network>

[46] Since the mobile internet service is designed for a data communication, the mobile internet service is disadvantageous over the mobile communication service such as CDMA and GSM. Considering the disadvantage, a DBDM terminal or a MBMM terminal supporting both the mobile communication service and the mobile internet service is used. In such case, the mobile terminal 200 includes the mobile internet modem 210 and a mobile communication modem 220.

[47] However, in accordance with embodiment, while the mobile internet modem 210 maintains the communication with the mobile communication service network 400 in order to receive an incoming call, a communication with the mobile internet service network 300 for the data communication is established selectively when required by a user. In addition, since the mobile internet service network 300 has a small service coverage compared to the mobile communication service network 400, the communication with the mobile communication service network 400 is frequently terminated when the mobile terminal 200 enters a shadow area.

- [48] When the mobile terminal 200 is unable to establish the communication with the mobile communication service network 400, the push data push_data cannot be transmitted via the IP push push_IP or the paging message push_paging even when a new push data push_data is generated in a push application server 10.
- [49] In such case, the integrated push service agent 250 connects to the paging controller 340 and informs the integrated push service server 100 of the mobile terminal 200 entering the network once connected to the mobile internet service network 300. the integrated push service server 100 searches whether the push information push_info that is not transmitted to the mobile terminal 200 exists to transmit the push information push_info as the IP push push_IP or the paging message push_paging. However, the push service is not provided in real time even in accordance with the embodiment.
- [50] In order to solve above-described problem, the integrated push service system further comprises the mobile communication service network 400 including a plurality of base stations and a SMSC, the mobile terminal 200 further comprises the mobile communication modem 220 for connecting to the mobile communication service network 400, the integrated push service server 100 transmits the push information push_info to the SMSC of the mobile communication service network 400 when the mobile terminal 200 is determined to be disconnected from the mobile internet service network, and the integrated push service agent 250 further comprises an SMS parser 254 for parsing the push information push_info when the push information push_info is received via an SMS push_SMS through the mobile communication modem 250.
- [51] In accordance with the embodiment, a real time push service is possible since the push information push_info may be transmitted via the SMS push_SMS even when the mobile terminal 200 is not connected to the mobile internet service network 300.
- [52] On the other hand, in a certain case, the push data push_data should be transmitted to the application 260 using a data service provided by the mobile communication service network 400 such as WAP (wireless Application Protocol) instead of the application 260 using the mobile internet service network 300. Typically, a method wherein a connection to a data network of a corresponding mobile communication service via the SMS is used. In such case, the integrated push service agent 250 may be configured to further include a mobile communication service interface. The integrated push service agent 250 further comprises the mobile communication service interface for controlling the mobile communication modem 220 to connect to the data network provided by the mobile communication service network 400, and may be configured to control the mobile communication modem 220 to connect to the data network of the mobile communication service network when the associated application ID app_ID of the received push information push_info designates the application 260 associated with

the data network of the mobile communication service network 400.

[53] <Method for providing integrated push service>

[54] Figs. 6 through 8 are diagrams illustrating a communication system of a method for providing an integrated push service in accordance with an embodiment of the present invention.

[55] First steps (S100 and S120) are carried out wherein a push information push_info including a push data push_data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data push_data and an associated application ID app_ID specifying the application for invoking the push data push_data is transmitted to an integrated push service server through a communication network.

[56] Thereafter, second steps S200 and S210 are carried out wherein a integrated push service server 100 transmits the push information push_info to the receiving mobile terminal 200 via an IP push through a mobile internet service network 300.

[57] Thereafter, third steps S500 and S600 are carried out wherein an integrated push service agent 250 resident in a memory of the mobile terminal 200 receives the push information push_info (S500) and invokes an application 260 compliant to the associated application ID app_ID to deliver the push data push_data.

[58] The embodiment is described in detail wherein the push information push_info is transmitted as a paging message push_message in order to provide the integrated push service even when the mobile terminal 200 is in an idle mode.

[59] First, the method for providing the integrated push service further comprises a fourth step wherein a presence server 130 detects the idle mode of the mobile terminal 200 prior to the first steps S100 and S120, the second steps S200 and S210 further comprises a first sub-step S305 wherein the push information push_info is requested to a paging controller 340 of the mobile internet service network 300 to be transmitted as the paging message push_paging when the mobile terminal 200 is determined to be in the idle mode, and a second sub-step S310 wherein the paging controller 340 broadcasts the push information push_info as the paging message push_paging through at least one RASs 320 and 211, and the third step S600 may be configured in a manner that the integrated push service agent 250 parses the paging message push_paging to extract the push information push_info.

[60] In accordance with the embodiment shown in Fig. 7 wherein the presence server 130 is not used, the third step further comprises a third sub-step (S700) wherein the integrated push service agent 250 transmits a reception acknowledge message ack_push to the integrated push service server according to the reception of the push information push_info, the second steps S200 and S210 further comprises a first sub-step S305 of requesting a paging controller of the mobile internet service network to

transmit the push information push_info as the paging message push_paging when the reception acknowledge message is not received and a fifth sub-step S310 wherein the paging controller 340 broadcasts the push information push_info as the paging message push_paging through at least one RASs 320 and 322, and the third step S600 may be configured to in a manner that the integrated push service agent 250 parses the paging message push_paging to extract the push information push_info.

- [61] After carrying out the third step S600, the integrated push service agent 250 may further establish a communication session with the integrated push service server according to the reception of the push information push_info.
- [62] Finally, an embodiment of the method for providing the integrated push service using the SMS wherein the mobile terminal 200 is a DBDM terminal that may connect to the mobile internet service network 300 and the mobile communication service network 400 and the mobile terminal 200 is not connected to the mobile internet service network 300 to provide the integrated push service in real time is described below in detail.
- [63] As shown in Fig. 8, the second steps S200 and S210 comprises a sixth sub-step wherein the push information push_info is transmitted to an SMSC of the mobile communication service network 400 when the mobile terminal 200 is determined to be disconnected from the mobile internet service network 300 and a seventh sub-step wherein the SMSC transmits the push information push_info to the receiving mobile terminal 200 as the SMS push_SMS, and the third steps S500 and S600 further comprises an eighth sub-step wherein the integrated push service agent 250 parses the received SMS push_SMS to extract the push information push_info.
- [64] While the present invention has been particularly shown and described with reference to the preferred embodiment thereof, it will be understood by those skilled in the art that various changes in form and details may be effected therein without departing from the spirit and scope of the invention as defined by the appended claims.

Claims

- [1] An integrated push service system comprising:
a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data;
an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push;
a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and
the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information,
wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.
- [2] The system in accordance with claim 1, wherein the integrated push service server or the mobile internet service network further comprises a presence server for detecting an idle mode of the mobile terminal,
wherein the mobile internet service network further comprises a paging controller for broadcasting a paging message for the mobile terminal through the at least one RAS,
wherein the integrated push service server provides the push information to the paging controller when the mobile terminal is determined to be in the idle mode through the presence server, and
wherein the integrated push service agent further comprises a paging message parser for parsing the push information when the push information is received as the paging message.
- [3] The system in accordance with claim 1, wherein the integrated push service

agent further comprises a reception acknowledge report manager for generating a push information reception acknowledge message according to the reception of the push information,

wherein the mobile internet service network further comprises a paging controller for broadcasting a paging message for the mobile terminal through the at least one RAS,

wherein the integrated push service server provides the push information to the paging controller when the push information reception acknowledge message is not received from the reception acknowledge report manager after transmitting the push message via an IP push, and

wherein the mobile terminal further comprises a paging message parser for parsing the push information when the push information is received as the paging message.

- [4] The system in accordance with one of claims 2 and 3, wherein the communication session manager establishes a communication session between the integrated push service server and the integrated push service agent by controlling the mobile internet modem when the push information is received as the paging message.
- [5] The system in accordance with one of claims 2 and 3, wherein the integrated push service server stores the push information when the mobile terminal is not connected to the mobile internet service network and transmits the stored push information when the mobile terminal is connected to the mobile internet service network.
- [6] The system in accordance with claim 5, wherein the integrated push service agent informs the integrated push service server of an entrance to the mobile internet service network via the paging message by connecting to the paging controller when connected to the mobile internet service network.
- [7] The system in accordance with one of claims 1 through 3, further comprising a mobile communication service network including a plurality of base stations and a SMSC,
 wherein the mobile terminal further comprises a mobile communication modem for connecting to the mobile communication service network,
 wherein the integrated push service server transmits the push information to the SMSC of the mobile communication service network when the mobile terminal is determined to be disconnected from the mobile internet service network, and
 wherein the integrated push service agent further comprises an SMS parser for parsing the push information when the push information is received via an SMS through the mobile communication modem.

- [8] The system in accordance with claim 7, wherein the integrated push service agent the integrated push service agent further comprises a mobile communication service interface for controlling the mobile communication modem to connect to a data network provided by the mobile communication service network, and controls the mobile communication modem to connect to the data network of the mobile communication service network when the associated application ID of the received push information designates the application associated with the data network of the mobile communication service network.
- [9] The system in accordance with one of claims 1 through 3, wherein the integrated push service server further comprises a transmission report manager for generating a transmission report including a result of a push information transmission, and transmits the result of the push information transmission to the push application server providing the push information.
- [10] A method for providing an integrated push service comprising steps of:
 - (a) transmitting a push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data and an associated application ID specifying the application for invoking the push data to an integrated push service server through a communication network;
 - (b) transmitting the push information to the receiving mobile terminal via an IP push through a mobile internet service network using the integrated push service server; and
 - (c) receiving the push information using an integrated push service agent resident in a memory of the mobile terminal, and invoking the application compliant to the associated application ID to deliver the push data.
- [11] The method in accordance with claim 10, further comprising (d) detecting an idle mode of the mobile terminal by a presence server prior to the step (a), wherein the step (b) further comprises:
 - (a-1) requesting the push information as a paging message using a paging controller of the mobile internet service network when the mobile terminal is determined to be in the idle mode; and
 - (a-2) broadcasting the push information as the paging message through at least one RAS using the paging controller, and
 wherein the step (c) comprises extracting the push information by parsing the paging message using the integrated push service agent.
- [12] The method in accordance with claim 10, wherein the step (c) further comprises
 - (c-1) transmitting a reception acknowledge message to the integrated push service server according to the reception of the push information using the

integrated push service agent,

wherein the step (b) further comprises:

(b-1) requesting a paging controller of the mobile internet service network to transmit the push information as the paging message when the reception acknowledge message is not received; and

(b-2) broadcasting the push information as the paging message through at least one RAS using the paging controller, and

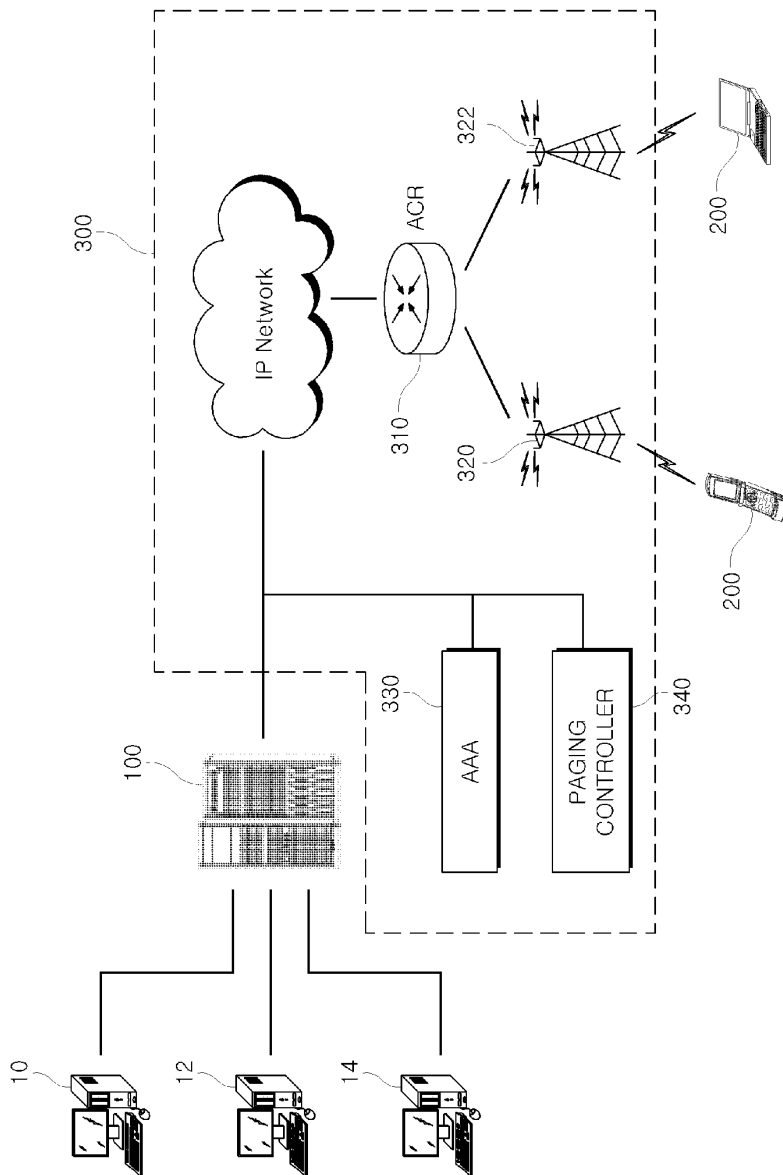
wherein the step (c) extracting the push information by parsing the paging message using the integrated push service agent.

[13] The method in accordance with one of claims 11 and 12, wherein further comprising (e) establishing a communication session between the integrated push service server and the integrated push service agent according to the reception of the push information after carrying out the step (c).

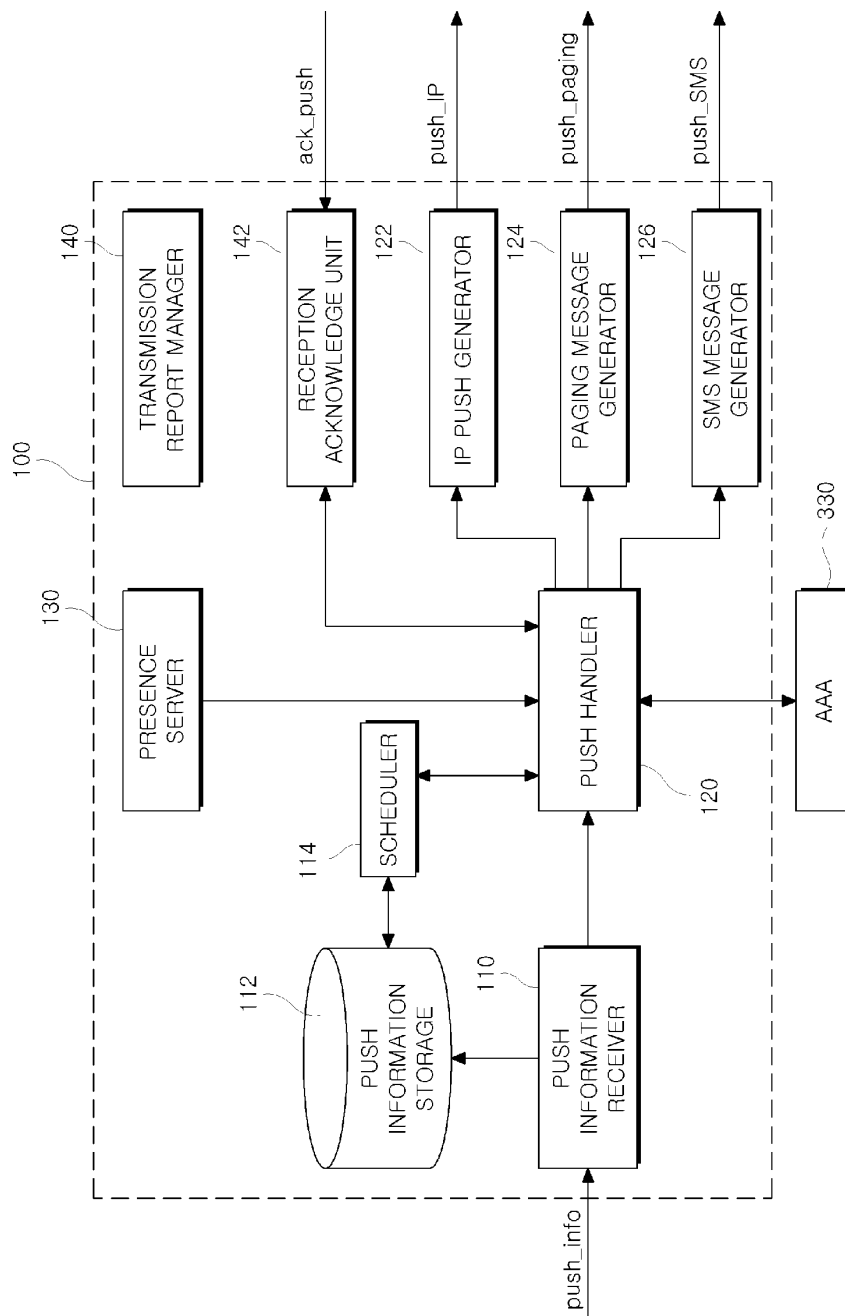
[14] The method in accordance with one of claims 11 and 12, wherein the step (b) comprises storing the push information when the mobile terminal is not connected to the mobile internet service network, and re-transmitting the stored push information when the mobile terminal is connected to the mobile internet service network.

[15] The method in accordance with one of claims 11 and 12, wherein the step (b) comprises:
(b-3) transmitting the push information to a SMSC of the mobile internet service network when the mobile terminal is determined to be disconnected from the mobile internet service network; and
(b-4) transmitting the push information to the receiving mobile terminal as an SMS by the SMCC, and
wherein the step (c) further comprises (c-2) extracting the push information by parsing the SMS by the integrated push service agent.

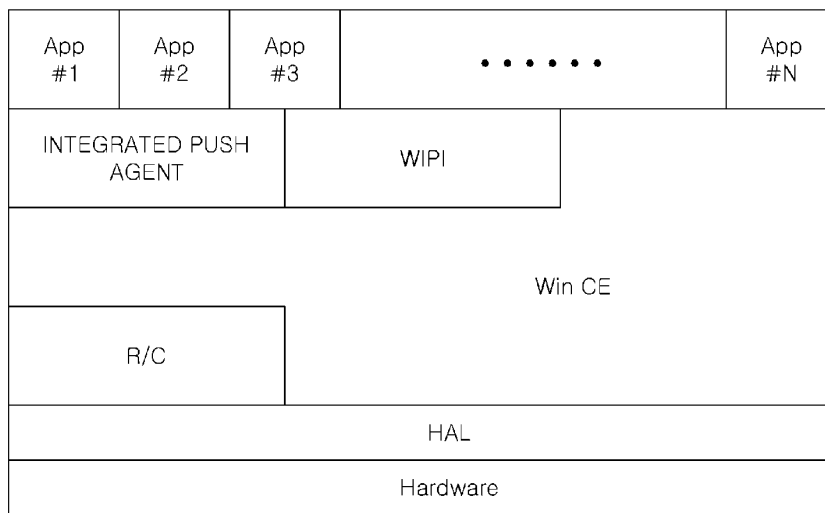
[Fig. 1]



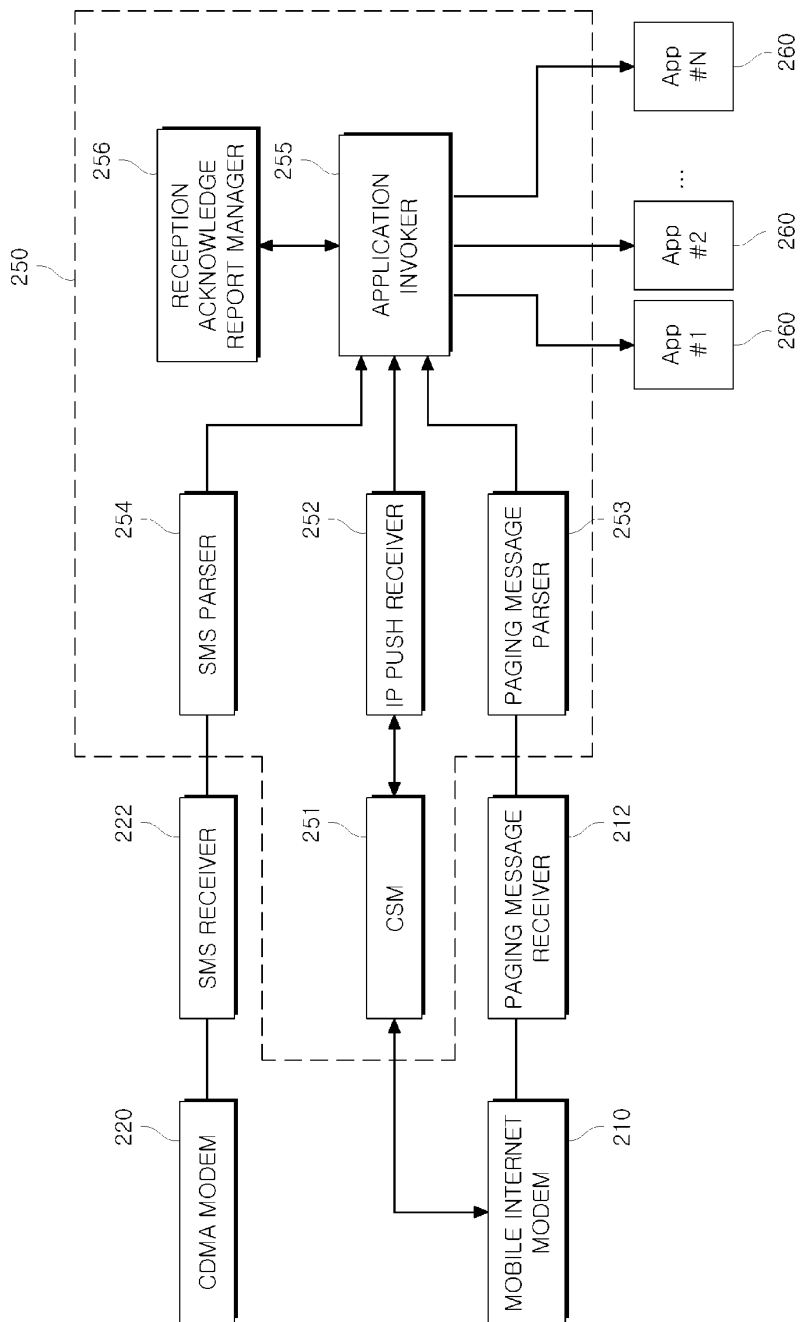
[Fig. 2]



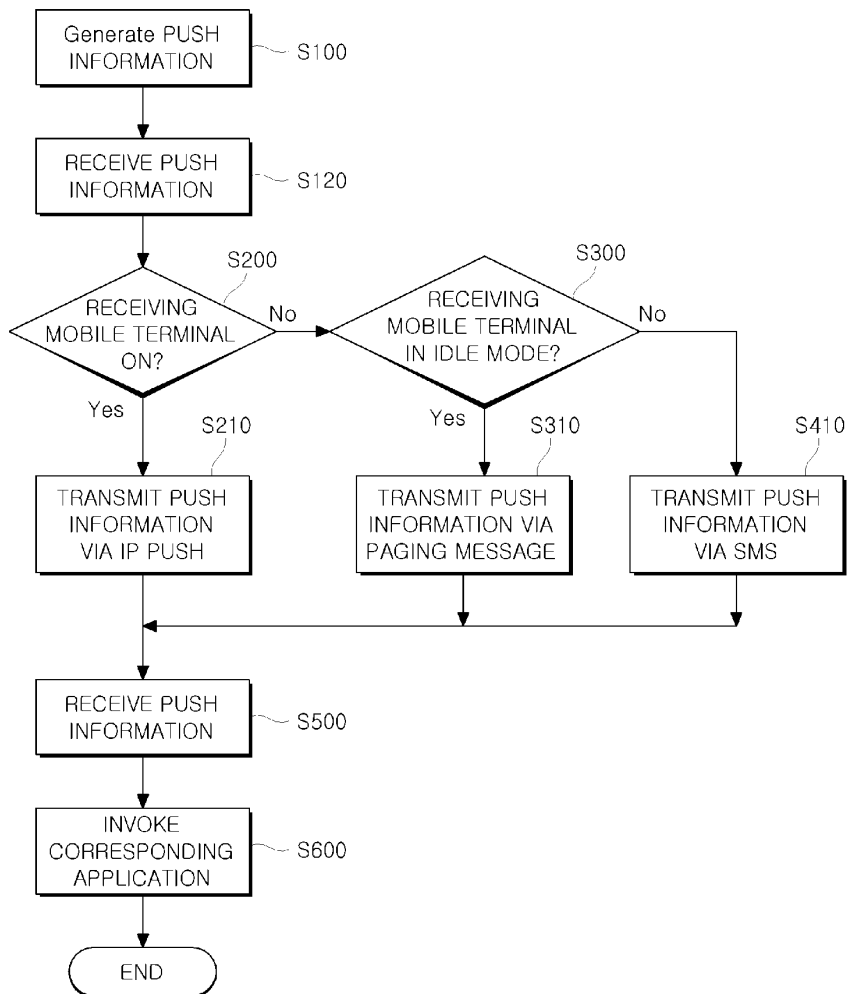
[Fig. 3]



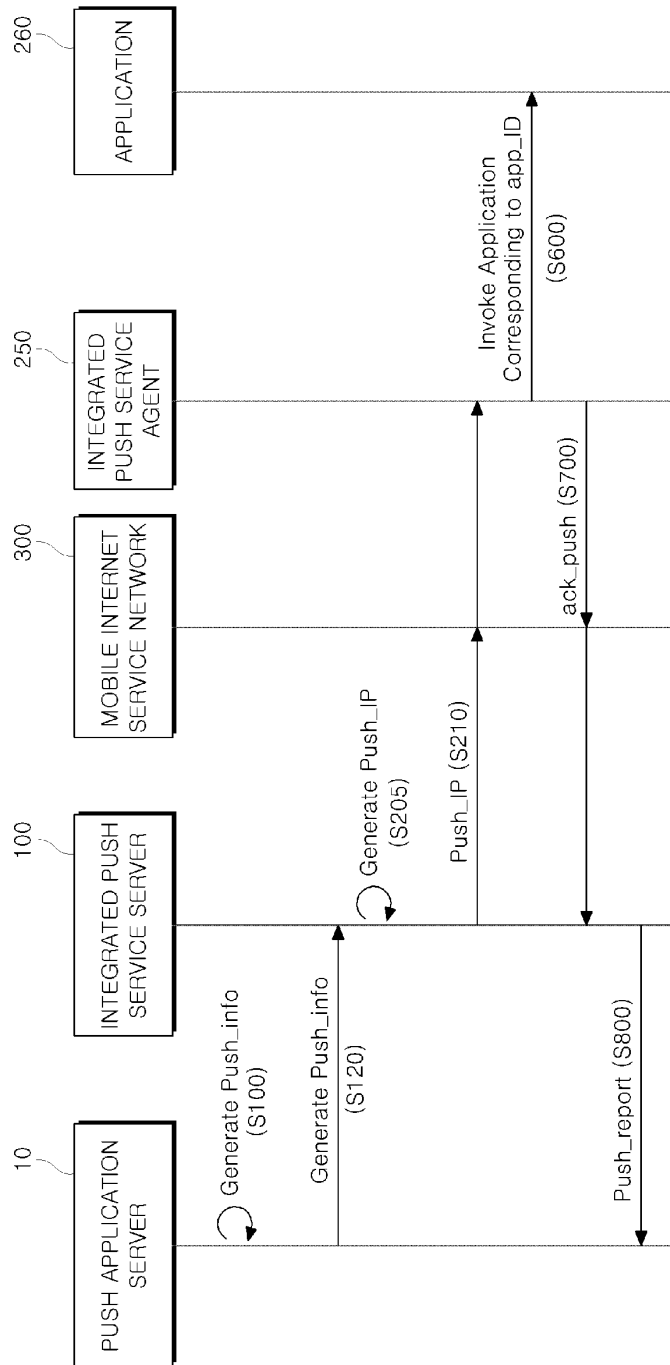
[Fig. 4]



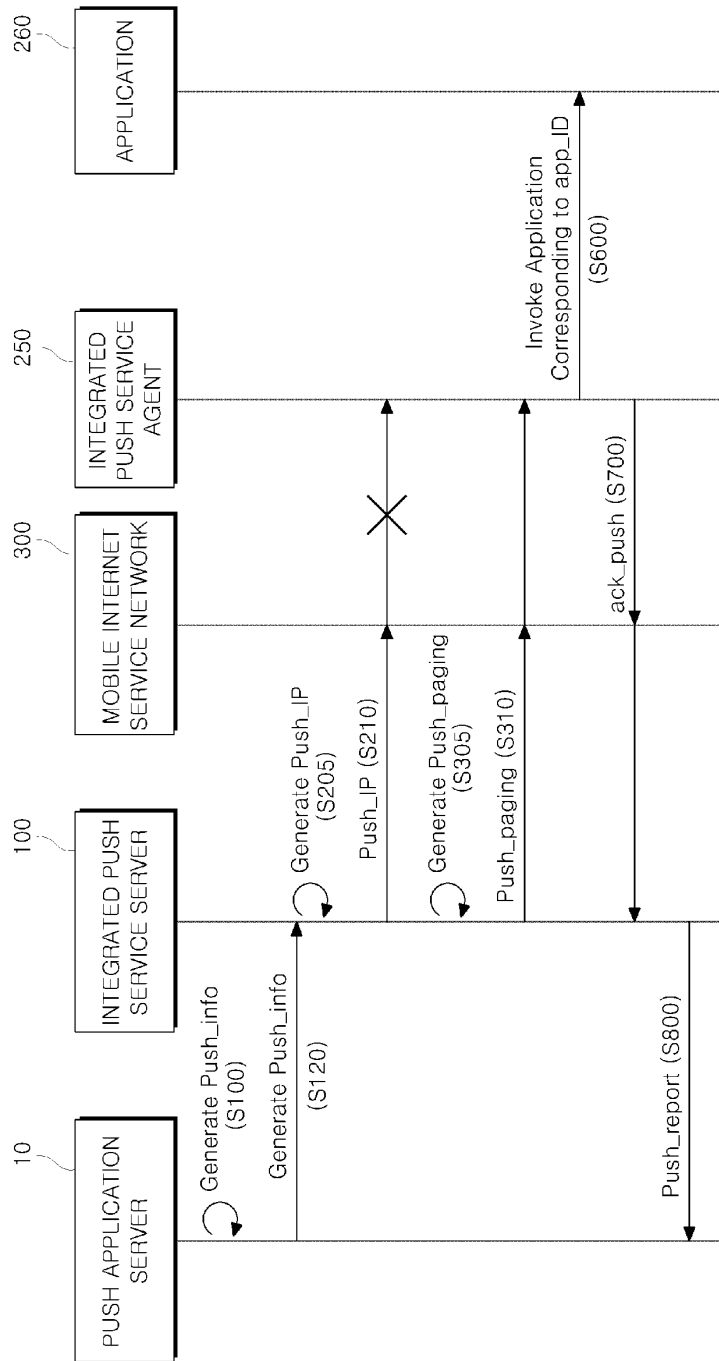
[Fig. 5]



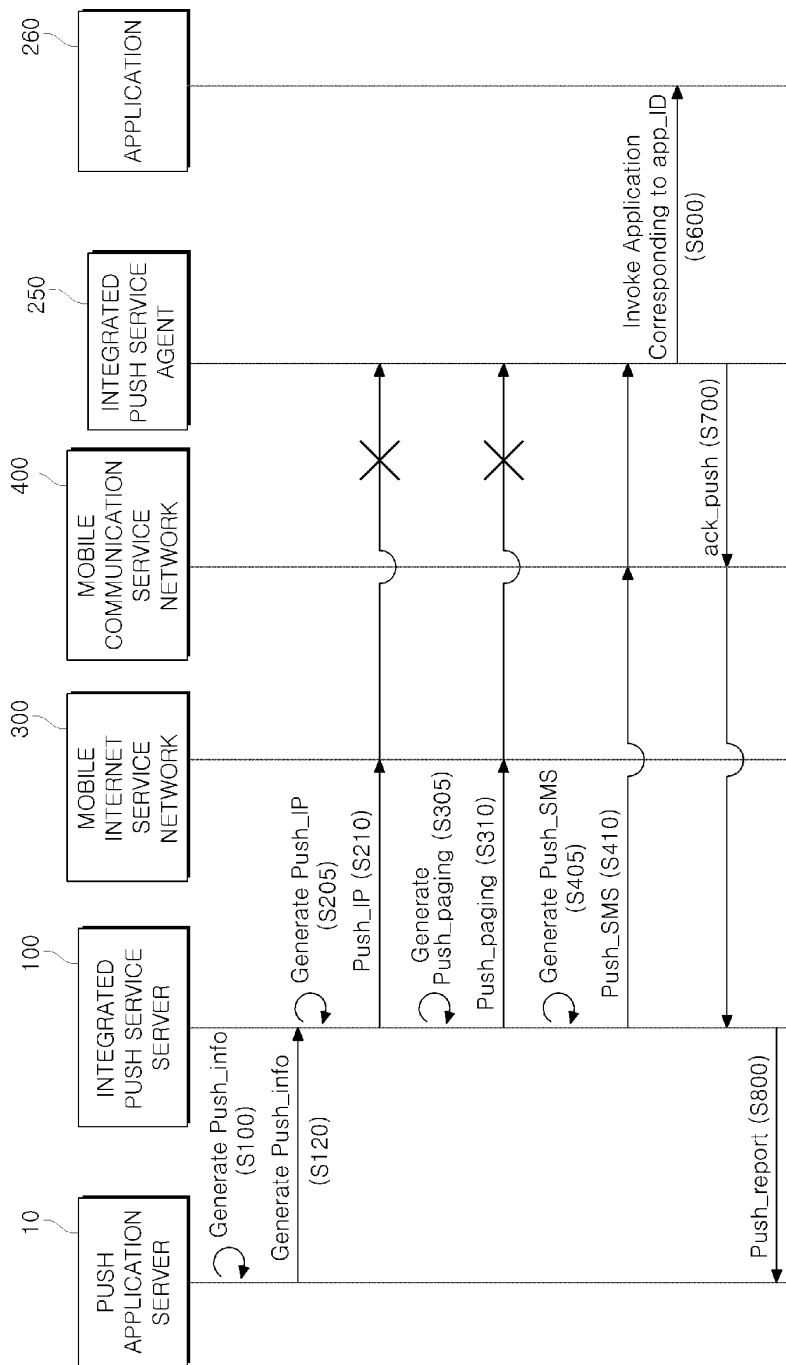
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/005155**A. CLASSIFICATION OF SUBJECT MATTER****H04Q 7/24(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : H04Q 7/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility Models since 1975

Japanese Utility models and applications for Utility Models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS(KIPO internal) "push, application, server, agent"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 06999991 B1 (Ikeda, H.) 14 Feb. 2006 See abstract, figures 1-2, claims 1-9, and column 6, line 53 - column 8, line 5	1-15
A	US 2002-0116472 A1 (Kalish, D. et al.) 22 Aug. 2002 See abstract, figures 1-2, claims 1-10, and paragraphs [0020]-[0032]	1-15
A	KR 10-2003-0037448 A (SK TELECOM CO., LTD.) 14 May 2003 See abstract, figure 2, claims 1-5, and page 3, lines 20-47	1-15
A	KR 10-2004-0045803 A (WIDERTHAN.COM CO., LTD.) 02 Jun. 2004 See abstract, figures 3-4, claims 1-4, and page 4, line 57 - page 6, line 9	1-15
A	KR 10-2005-0064905 A (LG ELECTRONICS INC.) 29 Jun. 2005 See abstract, figure 3, claims 1-3, and page 3, lines 1-15	1-15
A	KR 10-2001-0008959 A (SK TELECOM CO., LTD.) 05 Feb. 2001 See abstract, figures 1-2, claims 1-6, and page 3, line 11 - page 4, line 4	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

26 DECEMBER 2007 (26.12.2007)

Date of mailing of the international search report

27 DECEMBER 2007 (27.12.2007)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Kwang Sik

Telephone No. 82-42-481-8355

45



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/005155

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 06999991 B1	14.02.2006	None	
US 20020116472 A1	22.08.2002	W02003088064A1	23.10.2003
KR 1020030037448 A	14.05.2003	None	
KR 1020040045803 A	02.06.2004	None	
KR 1020050064905 A	29.06.2005	None	
KR 1020010008959 A	05.02.2001	None	



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	12/12/2024 03:32:15 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	12184700
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	68348121	AUTHORIZED BY	Michael Farjami
CUSTOMER #	106963	FILING DATE	01/17/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Gregory G. Raleigh

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 5006	E2024BBF33426140	Evan Gunderman

PRE-AUTHORIZED ACCOUNT	PRE-AUTHORIZED CATEGORY
500731	37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees); 37 CFR 1.21 (Miscellaneous fees and charges)

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2820	REQUEST FOR CONTINUED EXAMINATION (RCE)- 2ND AND SUBSEQUENT REQUEST (SEE 37 CFR 1.114)	800.00	1	800.00
TOTAL AMOUNT:				\$800.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	12/12/2024 03:32:15 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	12184700
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	68348121	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 16

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C 1C1C1_RCE_IDS_Dec_12_2 4.pdf	7	-	1135 KB
RALEP007C11C3C2C3C2 C1C1C1_RCE_IDS_Dec_1 2_24-TRAN.LET.pdf	(1-1) 1	Transmittal Letter	32 KB
RALEP007C11C3C2C3C2 C1C1C1_RCE_IDS_Dec_1 2_24-RCEX.pdf	(2-2) 1	Request for Continued Examination (RCE)	35 KB
RALEP007C11C3C2C3C2 C1C1C1_RCE_IDS_Dec_1 2_24-IDS.pdf	(3-7) 5	Information Disclosure Statement (IDS) Form (SB08)	1068 KB
AppendixH.pdf	28	Foreign Reference	1218 KB

AppendixT.pdf	57	Foreign Reference	2712 KB
9198117 File History.pdf	1060	Non Patent Literature	13081 KB
AppendixC.pdf	277	Non Patent Literature	3127 KB
AppendixM.pdf	220	Non Patent Literature	3132 KB
AppendixU.pdf	110	Non Patent Literature	13363 KB
AppendixAB.pdf	78	Non Patent Literature	5020 KB
AppendixAC.pdf	114	Non Patent Literature	8458 KB
AppendixAD.pdf	17	Non Patent Literature	1053 KB
AppendixAE.pdf	27	Non Patent Literature	8222 KB
AppendixAF.pdf	13	Non Patent Literature	290 KB
AppendixAL.pdf	92	Non Patent Literature	8820 KB
Request For Ex-Parte Reexam.pdf	209	Non Patent Literature	3132 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C 1C1_RCE_IDS_Dec_12_24.pdf	95FE4B759F297FFD2D2C0FA03BC88637A068B91E6F862A2FD E485560AF61FB9E1CDF7B7384E1164BB36745A2D3743D0BC8 914BA2DA6016D1F525A017558737D6
RALEP007C11C3C2C3C2C1C 1C1_RCE_IDS_Dec_12_24- TRAN.LET.pdf	7864428A93B09F831281C3BA8E96A4719B62174B37ABD9F5E A05438F45127D4DD9AD7429B07C4ABFA32E0001D5A3C95679 E306C2E6C799478E61E6EC707C5E25
RALEP007C11C3C2C3C2C1C 1C1_RCE_IDS_Dec_12_24- RCEX.pdf	C5AE3274CFAE0B0F460444C590583986B5D1432E3C42D2114 B720782A866DE133E21E2E4F7589E9DEDD34B15E706235FA5 C1D64CB54131197BACC5C651BC784B
RALEP007C11C3C2C3C2C1C 1C1_RCE_IDS_Dec_12_24- IDS.pdf	8E6F263CD5A299C22279630258C149FDDA8BD1BCC2F73054 ACC6BA0506D343696EE2E2F5932D735D05EEB5DBA6E5DA3F AFC6BF15D412D0BF19765C0C56EC63EA
AppendixH.pdf	E62F6283FD3D3BA315E5AF3F681603A42B4060D1EC381F645 0310B9F4ED016D1D7CFEA65B840B0E5EAD6A04D11585EDE5 D575A2C62BB27EA1FC6DB7239325F4A
AppendixT.pdf	A11D555D280C73A4DA82326D9CDAB7F14CB09849C021E1C1 A810C42E794419C558D4196A6B42A08238C0BF3506EA878444 CD038F549D7E7009118D4B6AE8972F

9198117 File History.pdf	7AC3C7A9F1F398041A645CE4CE4381B97F5347884E26906171 D0DFFF9A8CA4958C05018D1C7151C5B8DB3CB9886C0437D9 4E6F48EAC92E622987AA883583DDBB
AppendixC.pdf	1A2BDA311524CC99A74A7AB3EC2ED52842A29AA0AACC484 D094A7F57678D063187DABBE9EF5EF0E157217CF8A5A2B2B7 9736240981E3DBFA7A938F83F2AEFA3D
AppendixM.pdf	E1BEE303632161DD649D17B4698B646D7CAA48B99A12DF96 E4926923109E670264CCB28DEB650A33FFE5AB82B69068EF2 64B79AA7051ADD15C0508CAFB6BC18C
AppendixU.pdf	E9A4EE073871D2EE9E300210C81A8D45DACEDE872A7F98A8 439C0D273BEB0DA1D66BE4430250D895CEBF56F27BAA7CC D20100E2A760EAA7B41AF4FC824269694
AppendixAB.pdf	F23FBBF81ADA4AC23EA729352B40FC31C75F613CA23387587 0CD13A5CBAB472B02768C4AF249FA1F2A36152F60AA34B407 7190C5D0165EE39F8EA88F4CA08EA8
AppendixAC.pdf	6359A5E0F6F404837884877BF2A74D1C4512B72B3826E0E10D BB9C7A3B07A0F60B2013BB1A1D43336A479FB5FB4D448A3E1 E7C823CCC93086C841F549250FBE4
AppendixAD.pdf	7BF63EB748D6D8BE7AE7D336414AFFFA5C2B6DC3B2C576C FF2D0C132C3E4C35EEF1FDA1CF59AB373435CEE1C34C2523 2E8EAED10C4B0989A144470F4C440560D
AppendixAE.pdf	2AFFFE3CD638A284356E744FD5755AA578ABC46D7D5280F42 1527E17F7357E906D1E11F699F34887A26F83C94FEC6E21A5 C8842B8B4B21D640F02DD13D9D42AD
AppendixAF.pdf	9F840888C8ECE693834E72C8903CDCABB08BC94C632258932 6AF39CA55D41C9C6964315979B3ACFD4259C7E85C91FA9C8 17B5C0774706DD48E7AEFDEC512B5DA
AppendixAL.pdf	4009DFD7FDF7C1CD57463FDA2940A77A715CAFAB6831C651 9A3134833FB8FC70DB54892D85BB48785CB6045B2AD78E5CA C8A971439D054D0CACB72A5CD6EA2A3
Request For Ex-Parte Reexam.pdf	AA0B879B21E789BA081F423DB19F516A38D6735393612B3F5 E529AC1063C568F05D01D3F26A83DC35059354783232DCF34 B66D3D392E778DDC6605BDAC62F0EE

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

APPENDIX T

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 July 2006 (27.07.2006)

PCT

(10) International Publication Number
WO 2006/077283 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) **H04Q 7/22** (2006.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/FI2006/050032

(22) International Filing Date: 19 January 2006 (19.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20050067 20 January 2005 (20.01.2005) FI

(71) Applicant (for all designated States except US): **STREAM MOBILE OY** [FI/FI]; Tammasaarenlaituri 3, FI-00180 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HOUGHTON, Paul** [US/FI]; Helmitauluntie 13b, FI-02770 Espoo (FI). **REHTIJÄRVI, Pekka** [FI/FI]; Itälahdenkatu 13 A 32, FI-00210 Helsinki (FI).

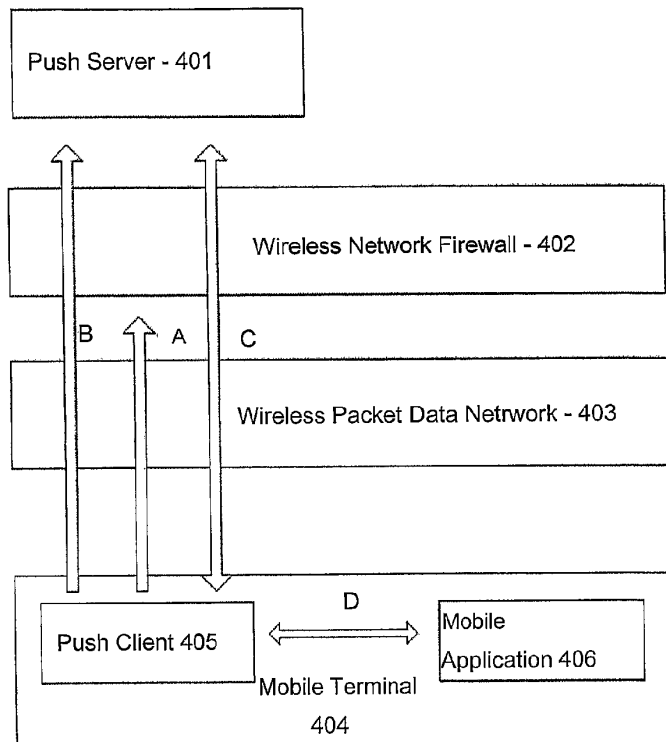
(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O. Box 148, FI-00121 Helsinki (FI).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PUSH MESSAGING COMMANDED METHODS AND DEVICES



(57) Abstract: A server outside a wireless network security entity is adapted to push messages to a mobile terminal located in the wireless network and thereby cause programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message thereby presenting a new application view to the user of the mobile terminal. The mobile terminal is provided with means, such as software, which initiates and maintains contact with the server using Internet technologies. This mobile-initiated permanent connection allows the server to pass or push messages from outside the operator's firewall to the mobile terminal at any time.

WO 2006/077283 A1



Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *of inventorship (Rule 4.17(iv))*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *with international search report*

Title of the invention

Push Messaging Commanded Methods and Devices

Field of the invention

The invention relates to techniques for launching applications on a mobile terminal.

Description of the Related Art

The Internet is a collection of networks which exchange messages using IP protocol (Internet Protocol) and associated protocols which run on top of IP such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Gateways between IP networks automatically route and transmit information over primarily the IP4 and IP6 protocols between two or more end points on any of the connected fixed and mobile networks. Each of these networks may also include or run on top of other network transport protocols such as ATM (Asynchronous Transfer Mode) or a wireless protocol which in turn carry the IP packets over that section of the Internet.

Currently, the most common method of starting applications on a mobile terminal is to manually launch them by clicking on an icon or selecting a menu item. If the application, dynamically loaded program module or user interface feature is already launched, these applications must also be manually commanded by the user to change state to display newly available information provided by a telecommunications network. Some applications are also launched automatically when the terminal is started. This automatic start includes both applications that were installed on the phone before delivery to the customer including the basic terminal operating system software and programs installed by service providers and users and which by various means ask the terminal software to start them automatically after the terminal is powered up.

Remote launch to a known state as specified in a network command of programs on mobile terminals is supported in various telecommunications standards. Voice Over IP (VoIP) and other multimedia sessions can be started remotely using Session Initiation Protocol (SIP). Wireless Application Protocol Push (WAP Push) is another standard for launching programs on mobile terminals based on remote events. Java Mobile Information Device Profile (MIDP) and various native mobile terminal operating systems also support remote application launch based on receipt of a text message (Short Message Service,

SMS) or incoming Internet (IP) packet of information to a designated communications port number. However it is important to note from an economics and practical service deployment standpoint that each of these technologies either requires payment to the mobile network operator for sending an SMS or privileged access to the mobile phone from inside the operator's firewall in order for IP data to actually reach the phone.

Mobile phones and similar mobile communication devices were originally not permanently connected to the Internet. Instead, for the transmission and display of visual information they have relied on different telecommunications standards and proprietary communication systems such as SMS (Short Message Service, also known as text messaging) and MMS (Multimedia Message Service), which were built into mobile terminals.

Various techniques have been proposed for remotely commanding applications on a mobile terminal using push technologies:

US20020183051 relates to remote application management of a wireless device.

US20030208602 relates to pushing data in an internet protocol network environment.

US20010020255 relates to remote control and interaction with a mobile run time environment component.

US6687743 relates to client server communications for a mobile computing device.

US6779019 relates pushing information from a host to a mobile data communications device.

US6701378 relates pushing information from a host to a mobile data communications device.

US6463464 relates pushing information from a host to a mobile data communications device.

US6463463 relates pushing information from a host to a mobile data communications device.

US6389457 relates pushing information from a host to a mobile data communication device.

US2004122907 relates to secure interaction between a mobile client device and an enterprise application in a communication system.

WO0195695 discloses a system for wireless push and pull based services.

US2002187775 discloses a WAP service personalization, management and billing object oriented platform.

US2003106022 relates to outputting dynamic local content on mobile terminals.

US2004185834 discloses a method for enabling IP push capability to wireless devices on a wireless network.

US2002174184 shows a mailbox access mechanism using SMS push and WAP technologies on mobile terminals.

WO02077842 shows a push method for delivering data to mobile device.

Wireless Application Protocol Forum, Ltd., "Wireless Application Environment Specification, Version 2.0", Version 7-Feb-2002, 2002.

www.wapforum.org.

Sun Microsystems, Ltd., "The MIDP 2.0 Push Registry", Network and Timer MIDlet activation. developers.sun.com/techtopics/mobility/midp/articles.

Nokia, Ltd., "SIP Session Initiation Protocol", Forum Nokia 2005. www.forum.nokia.com/main/0,6566,1_44,00.html.

Nokia, Ltd., "SIP Frequently Asked Questions", Forum Nokia 2004. SIP_FAQ_v1_0_en.

RFC 3261, "SIP: Session Initiation Protocol", 2002. www.faqs.org/rfcs/rfc3261.html.

Push technology is characterized by the server proactively sending documents or information to a client or user. E-mail (Electronic mail) is actually a special kind of push technology that has been prevalent for a long time. The first and most common general category of mobile content push technologies is SMS (Short Message Service) based technologies. SMS and MMS (Multi-media Messaging Service) are the most common forms of "push" messaging in the mobile industry. These store and forward messaging systems run by mobile telecommunications operators push all or part of the data to the mobile terminal over closed telecommunications signaling networks such as SS7 (Signaling System Seven). These signaling networks are closed; they are not part of the Internet. Each operator controls and encrypts this traffic, charging high prices for their use and limiting their use and usefulness.

FIG 1 shows a generic implementation known in the art for pushing launch and operational commands to applications on mobile terminals. Email, MMS, WAP (Wireless Application Protocol) pages, and custom application

data are delivered through existing telecommunications infrastructure to a mobile terminal using SMS as the push messenger medium. First, push server software 101 delivers the notification to an SMS Gateway 102, as illustrated by the arrow A. The SMS Gateway puts the actual SMS push message in either readable text or compressed binary format into the telecommunications signaling network 103, usually SS7, which delivers it in a store and forward fashion often involving several intermediate steps to the mobile terminal 104, as illustrated by the arrow B. The mobile terminal standard software 105 decodes header information in the SMS and based on the fields in this binary SMS header not visible to end users, delivers this as a normal SMS, an MMS, WAP pages or a custom application command action (C) to the indicated mobile application 106, launching the application if necessary. These custom application launches by SMS require the application to first register itself with the mobile terminal in order to receive SMS push message command events.

Besides a high price per message, SMS messages cost different amounts depending on where the sender and receiver are located. In some countries the sender pays for the message, in other countries the receiver pays. Computers called Short Message Service Center (SMS-C) nodes and owned and managed by each mobile operator deliver SMS messages. In many cases, if the sender and receiver are on different continents the operators do not even offer message delivery. Two operators must negotiate, sign and implement a legal contract known as an interconnect agreement before messages flow between SMS-Cs and thus between mobile terminals on different operator networks. Since not all operators have such contracts with all other operators, this limited connectivity also means that commanding mobile applications based on any SMS technologies can not be delivered on a global basis. For example an SMS-based remote application command server run from a European telecommunications operator will face the practical limits of incomplete operator interconnect agreements when pushing application commands to their North American and Asian customers. Also, because of the billing models in different countries are also variable, high costs and delays when roaming, it is difficult to develop reliable global application command using SMS-technologies. For example, such SMS delivery arrangements to all operators within one country or in multiple countries usually rely on expensive arrangements with middlemen or brokers that route computer-originated mes-

sages to phones in many locations. Even the best of these such middlemen still do not offer global coverage to all countries.

A newer telephone company standards-based method to delivery content and command applications which have not been explicitly requested by the user of a mobile terminal is WAP Push. WAP Push technology relies on an SMS to start the message delivery process. Both SMS and WAP Push using SMS can be used to command applications on the phone. Java applications on mobile terminals can also register themselves to be launched upon receipt of an SMS and then interpret the contents of the SMS as a type of launch command or launch content. But in all these cases operators continue to control the push medium and charge money for each push event. This operator control of content on mobile terminals is known in the industry as the "walled garden" approach.

SMS messaging standards include the ability to send binary messages to an application installed on the mobile terminal. Parameters in the message header and applications in the mobile terminal are matched by the mobile terminal at delivery time and the selected application receives the pushed SMS contents, starting the application if it is not already running. This is a standard software feature installed on the phone at time of manufacture as part of the mobile terminal's operating system.

The cost of using such an remote command capability is quite high-the cost of an SMS each time the program is commanded, thereby limiting the broad utility of this feature for all but a telecommunications operator supplying the service only to their own customers. These standard SMS-based telecommunications technologies for push application remote command are all thus limited by economics in both the frequency with which they can be used and the breadth of market which they can reach. Also due to the low speed of SMS delivery as a store-and-forward messaging system, it can take a long time for the application to launch to a known state based on a remote command thus making this unsuitable for use in any real time or time critical situations.

A further limitation of existing SMS remote command technologies is the inability to prioritize, select and deliver messages in different ways to a user based on their current situation, location and individual preferences. More important application command events may be buried behind several less important events causing critical items to be missed or confused. A user can not select with these SMS-technologies not to be notified, or to be notified in a

more polite manner, or to go ahead and start to a known state or change the visible operating state of the application without politely asking in some circumstances. And a user can not specify that they would like to only receive or receive a request for permission to execute a certain category of application command events during a given period of time.

A second general category of mobile push technologies is IP-based technologies. These include IP connections initiated from the server and IP connections initiated from the client. Server-initiated push connections are the most commonly described. These solutions require IP communication with software installed on the terminal and a server which has been notified of the IP address of this terminal. The server then, when a push event is desired, initiates a connection to the terminal and delivers information to it which software in the mobile terminal can then act upon, most commonly to notify the client of an incoming email message. For reasons described below, these push technologies are not generally used on mobile terminals but are more commonly used between one server and another as in the SMTP mail transport protocol when delivering email. Similar methods are also used for launching, commanding and communicating with applications on servers and in some cases on mobile terminals.

There are, however, difficulties with commanding applications on mobile terminals based on receipts of an IP packet when there is not an already established IP connection between a mobile application program module or feature and the command push server. In practice, mobile terminals are on sections of the Internet which are most commonly behind a firewall or gateway server device creating a controlled mobile network. This difference from the above-mentioned server-to-server push technologies is non-obvious when reading standards and results in many server-to-client and server-to-mobile-terminal push technologies which in practice do not work because of firewalls protecting the mobile terminal. Thus firewall and mobile gateway devices at the connection between the security-controlled mobile network and the more public Internet frequently restrict computing devices such as servers on the public Internet from directly contacting mobile terminals. Additionally, IP connection and security techniques, such as network address translation, firewalls and gateways, may hide the actual address of the mobile terminal further complicating direct connection from an Internet computing device. Further, the mobile

terminal may be unavailable at any given time making such messages undeliverable.

The public telecommunications operator, company, organization, or private individual setting up a mobile Internet space with one or more users uses the above-mentioned firewalls, security devices and gateways to protect the mobile terminals from hostile or unwanted contact common on the public Internet. They may also do so to reduce background traffic, protect their control over this space and thereby limit outside or undesired service providers through technical connection policies set in the firewall or gateway device. The result is, if a fixed or mobile computing device from outside the controlled mobile network tries to contact a mobile terminal inside the controlled mobile network, the connection is not permitted unless the organization or individual controlling the firewall or gateway server device makes an exception to their security policy and explicitly allows the connection. Instead, in standards-based mobile Internet telecommunications, an intermediary computer with privileged access from inside the firewall to the mobile terminals is used. These server computers such as a telecommunications operator SIP Server or WAP Gateway is used to control and deliver messages and store messages when the mobile terminal is unavailable and deliver them on the senders behalf, possibly later then the terminal becomes available, or to forward them to a different gateway device, for example if the user is roaming to a different controlled mobile network.

The most common solutions to accessing mobile terminals subject to this mobile network restriction are to either make an agreement with the public or private network operator removing the security restriction on a specific outside server contacting mobile terminals, or to move the server inside the controlled network. In the common case of a public mobile network operator, the state of the art and most common solution is to sell the server and associated software to the mobile operator so that they can provide the service to their customers. Both of these solutions require time, effort and often large financial commitments. And they must be done for each and every restricted mobile network and operator in a given market to achieve universal access to a service requiring server-initiated IP push. Achieving such universal penetrations on all operators in all markets is not practical. However for those operators with whom such a relationship has been established, mobile application launch and command with standard IP technologies is thus possible.

Client-initiated mobile IP connections are less common in mobile terminals. These are also not part of state of the art mobile application command telecommunications standards. Client-initiated IP connections involve installing more complex software on each mobile terminal and having these devices initiate contact to a server on the public Internet. These connections generally operate in a polling or "content pull" manner, connecting intermittently to the server to ask if any new information is available. Mobile email is a common example of this approach for content download. While the result appears to be push to the end user when they are notified several minutes later of the incoming email, they were not notified immediately by the server when the message is available as in true push technologies. The network settings of the mobile terminal may also need to be adjusted to permit this since Internet access through default gateway devices may not permit this type of connection.

FIG 2 shows a generic implementation known in the art for pushing launch and operational commands to applications on mobile terminals using Internet technologies. Symbian, Linux, Microsoft and other mobile IP terminal operating system software all include application launch capabilities based on this socket-based triggering mechanism. Each mobile application 205 has a fixed IP port number such as TCP/IP or UDP/IP port numbers. When a remote program such as a push server 202 sitting inside the operator's firewall 201 and with permission to contact ports on the mobile terminal 203 sends an IP packet to the terminal (A), the IP terminal software 204 routes the packet with it's commands or application-specific data to the mobile application 205 (B), launching the application if it is not already running. Java applications sitting on top of the lower levels of IP terminal software can be similarly launched based on Java MIDP 2.0 and later "push registry" settings.

FIG 3 shows the same steps A and B shown in FIG 2, however the push server 301 may be located outside the firewall 302 because the wireless network firewall has been configured by the mobile network operator to allow communications from that particular push server. This allows IP traffic to flow from the push server 301 to the IP terminal 303 and be internally routed 304 to the mobile application 305.

The important point to note in the standard methods shown in both FIG 2 and FIG 3 is that the permission of the wireless network operator is required to either locate a push server within their firewall or open a firewall hole to a given push server. This permission is in practice expensive for an arbitrary

push server to achieve with a given operator. It is virtually impossible to achieve with all mobile network operators in all markets. A viable market alternative to the state of the art methods shown in FIGURES 1, 2 and 3 for the mobile terminal and push server to initiate and maintain contact for push application launch and configuration commands without explicit arrangements with each mobile network operator is thus needed and described in the invention below.

Once such an IP connection is established between the server and one or more mobile terminals, the connection can be used to transfer messages to the mobile terminal. The most interesting such messages for the present invention are event trigger messages to launch or command a mobile application. Other interesting uses include the sending of data files, new applications and applications updates to replace or improve installed applications. These messages, while simply inexpensive IP traffic can if sufficient in number result in significant costs or the user perception of their incurring significant data traffic costs. For this reason it is also desirable to route such information including application updates, bug fixes, additional features, additional application data including multimedia, vector graphics, text and executable code through the lowest cost available network connection. Further it is desirable but not generally possible to automatically do so only during those times that a lower cost network connection is available as through the presence of a broadband wireless access device.

Numerous mobile applications such as games and productivity software are now included with new mobile terminals. They can be used to perform an endless variety of tasks, some of which involve interaction with elements outside the mobile terminal, for example on desktop computers, servers and other mobile terminals which are also connected to the Internet. The process of a user manually performing actions such as starting the mobile application to become aware of the state of remote computers and terminals is referred to as pull because a user action triggers or "pulls" the information for display to the phone.

Multimedia audio and video presentation applications, Voice over IP (VoIP) communications, multimedia interaction applications, games including games which involve other player and automated server actions such as game events and challenges from other mobile terminals, mobile business process applications, real time back office connectivity applications and corporate mes-

saging programs are examples of areas where mobile terminal applications benefit from the ability of server placed arbitrarily on the public Internet having the ability to initiate the display of or remotely configure the view presented by an already running program on a mobile terminal at any time. Due to technical limitations of the terminal and user preferences, it is generally not possible for a mobile terminal to support multiple such large or resource-intensive applications running continuously. Therefore there is a need for a more general solution to automatically install, update, provide data to, launch and configure these applications from the background on mobile terminals on any mobile network.

Commanding an application on the mobile terminal, launching an application with parameters specified in the launch message so as to view specific information after the program starts, changing the current view of an application which is already running, pushing or pulling new information into an application so as to change what is presented to the user are all referred to herein as changing the state of the application. This application state change process generally requires personal initiative and several manual and cumbersome steps and decisions on the part of the user: opening the application or changing the view of the application, selecting and then examining the content to see if any of the changes are of interest. Because of the limited size, network bandwidth and user interface of mobile terminals, performing these steps is significantly slower on a mobile terminal than performing the same actions on a larger computer. The process of checking if an application should be launched now because new and interesting Internet information might be available is therefore less interesting to mobile terminal users than on a larger terminal because of the limited capabilities of the mobile terminal to rapidly display many alternative content formats. This frustrating or slow user interface with for example small buttons, touch screen or relatively slow interface response on the mobile terminal is one of the reasons there is commercial need for eliminating the user steps and push commanding the mobile application remotely from a server only when new and interesting information is available.

Given the shortcomings in the prior art, there is a need for a method whereby a computer on the Internet can rapidly and at reasonable cost be permitted to at any time initiate control of one or more applications on an individual's mobile terminal to deliver through that mobile application real time in-

formation, interactivity and rich media content, regardless of which mobile operator is being used and where the mobile user happens to be at that moment.

Brief description of the invention

An object of the present invention is a new technique for providing a push-type command of applications on a mobile terminal by a remote server computer. The object is achieved by the invention is characterized by what is stated in the attached independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

In a preferred embodiment of the present invention is a system and method for a server placed freely on a connected network outside the wireless network firewall or other corresponding wireless network security entity, to push messages to a mobile terminal located in the wireless network and thereby cause programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message thereby presenting a new application view to the user of the mobile terminal. The mobile terminal is provided with means, such as software, which initiates and maintains contact with the server using Internet technologies, thereby avoiding cost, latency, contractual and firewall penetration issues of the server contacting the mobile terminals by telecommunications messaging or Internet technologies. This mobile-initiated permanent IP connection allows the server to pass or push messages from outside the operator's firewall to the mobile terminal at any time. If the server would attempt to use IP to contact the mobile device directly, the attempt would fail due to the firewall(s).

In an embodiment of the invention, the mobile terminal maintains contact with the server by periodically testing the connection with a suitable keepalive message, a "ping", which resets timers in intervening operator stateful firewalls and/or NAT (network address translation) firewalls. The mobile terminal may also automatically re-establish the connection when the connection gets broken and adjust its connection settings based on past experience with failure to connect and such broken connections in a given mobile network.

In an embodiment of the invention, the push messages may include, for example, a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface feature of the terminal such as an application which is part of the basic terminal software or and an additional installed application beyond the base software supplied with the mobile termi-

nal. In response to receiving such a message, a mobile terminal may spontaneously open the application, dynamically loaded module or user interface feature of the terminal thereof to a designed application view or location, present new information of the availability of new information, a new feature or operating state. If such application, module or user interface features is already operating in the mobile terminal, the action of such a message would instead stimulate the application or user interface feature to present itself to the foreground of the user interface and change state as specified in the application-specific message received from the server. In further embodiments of the invention, push messages may include, for example, messages triggering the mobile terminal to play a sound notifying the recipient of the application command or state change, or display notification providing event information from which the user may select or decline to display the application.

Note that in some cases the packaging of mobile applications involves combining multiple applications delivered in a single bundle or application suite preinstalled or later installed to the mobile terminal. Commanding the display of an additional, more resource-intensive user interface feature such a rich media, or highly interactivity modes within the same bundle of applications or application features as for example by explicitly or implicitly loading or calling an additional library such as a user-interface related code or other embodiment of an application on a mobile terminal within the same application based on push event messages recently received from an IP connection is simply an alternative packaging of this same invention. For brevity herein, this type of commanding of a new user interface modes or view to appear within the same application suite is considered and discussed as the commanding of a new application since the packaging of rich user interface features and program modules within a bundle or separately is a relatively minor detail in the embodiment of the invention.

The cost for a user's mobile terminal to maintain a connection to the push server and receive such messages over mobile Internet connections is minimal, thereby solving the problem of some mobile information services not being economic to offer. The advantages are: all the convenience of standard push services such as SMS-based application launch and command together with the mobile network-independent and economic benefits of placing the server outside of any single operator's network and of the service provider not having to pay an operator or operator middleman per command event.

IP push messages utilizing the principles of the invention are delivered rapidly, bypassing the public and often crowded SMS, MMS, WAP Push and email store-and-forward mechanism within an operator and between operators. This guarantee of very rapid event push provides usability benefits to users which may be then designed into the mobile applications. For example the ability to expect prompt delivery allows modification to interactive mobile application system design. The mobile process surrounding the application can be changed such that a user on one mobile terminal may take actions which result in the initiation of a push event to a user on a second terminal and then wait for a short time for the second user to respond after the launching or commanding to return to be the focus of user interface attention their copy of the same, similar or complimentary mobile application function involving Internet communication directly or mediated by a server between the two mobile applications.

The advantages of performing push service application command in accordance with the present invention include the ability to run such a service from outside the mobile operator's firewall and gateway devices, skip the overhead charges like per-message SMS fees normally associated with "mobile push", and make it easy to create mobile applications as web pages, therefore usually without programming. Thus, push application command services according to the invention can be modified from existing or newly designed mobile applications, modules and application features simply by creating an application command, module or feature entry point compatible with the embodiment of the push client. This embodiment can be, but is not limited to, a separate application, operating system background process or application module bundled in a suite with the mobile application and kept running such that it may receive IP push events and command applications, modules or significant application features.

These messages may be routed automatically to a nearby computing device with faster or less expensive network connectivity such as a broadband access point, server or workstation in the proximity of the mobile terminal. Both mobile terminal and access point must be equipped with a wireless communication network such as RFID, Bluetooth, ultrawideband, Zigbee, Wi-Fi, Wi-Max or other personal area, local area, metropolitan area or large area network. This ability embodied in the invention alleviates speed and economic problems that affects the present-day mobile messaging solutions which are either limited in bandwidth or cost based on volume of use. When in proximity to a more

capable network, if a connection can be established to this alternative broadband network access point, it is used preferentially and intelligence normally located in this broadband access point would route messages received on behalf of the wireless terminal to and from the server. Further, the availability of a broadband access point would be notified to mobile terminal application software and server alike allowing either to initiate bandwidth intensive operations such as application update and application data update.

IP push command messages may be triggered either by events which the server is aware of, or events which a similar mobile application on another mobile terminal is aware of and which that push client makes the server aware of, the server in turn initiating a push command event. Such client-side events of which the server is informed for the possibility of delivering new web services include the making, receiving, and termination of telephone calls, the transition from presence-to-absence or absence-to-presence of other devices in a geographical area, metropolitan area, local area or personal area wireless communications network, mobile terminal creation of photographs video audio or other media, mobile terminal presence of files matching a given filtering criteria, changes in internal state of electronic equipment, taking of measurements, processing of such measurements to see if they match certain criteria, video game actions or events, application calculation events and messaging actions. In some cases a separate server such as a telecommunication service server, gaming environment server, and original equipment manufacturer device or business information system may notify the server directly of events or messages to be sent using an external application programming interface (API). Such a device connected by external API may also receive information including the results and responses of messages which the user has replied to by terminal software or web page interaction.

The invention provides content and application producers with a cost effective, network-independent and device-independent service for the rapid creation and distribution of interactive information alerts and Internet launch-at-will and present-when-needed features for their users.

The invention provides techniques for launching and changing the operating state such as information currently presented to the user of applications on a mobile terminal at will by a server computer and without the need for any additional action by the recipient, and more specifically to a system, method and program for sending, receiving and acting upon messages sent to a mo-

mobile client device over a packet switched data network for the purpose of initiating application launch, application command, module or feature display and user direct or indirect user interface state change based on server-side events and mobile terminal events including user interface events, phone calls and network proximity events, and local resource changes.

Brief description of the drawings

In the following description, reference is made to the accompanying drawings which form a part hereof, and which illustrate several embodiments of the present invention. In the drawings:

Figure 1 shows an implementation known in the art for pushing information including commands to an application through existing telecommunications SMS infrastructure to a mobile terminal and if necessary launching the application;

Figure 2 shows an implementation known in the art for pushing information including commands from inside the mobile network firewall to an application to a mobile terminal and if necessary launching the application;

Figure 3 shows an implementation known in the art for pushing information including commands from outside the mobile network firewall through a firewall hole opened by the mobile network operator to an application to a mobile terminal and if necessary launching the application;

Figure 4 is a block diagram illustrating an exemplary implementation of the system for pushing mobile application launch commands to a mobile terminal based on server side events in accordance with one embodiment of the present invention;

Figure 5 is a block diagram illustrating an exemplary implementation of the system for a wire terminal with an alternative broadband connection to use the alternative broadband access point for receiving push messages including launch events, application updates and data updates;

Figure 6 is a flow chart illustrating an exemplary process by which the mobile terminal maintains an open path for network communication with the server (6A), keeps the connection to the server open and tests the integrity of the connection while automatically reestablishing the connection as necessary (6B), responds to messages from the server (6C), and notifies the server of locally monitored events on the mobile terminal (6D) in accordance with one embodiment of the present invention;

Figure 7 illustrates an example of a "COMMAND PUSH" procedure;

Figure 8 illustrates an example of a "COMMAND PUSH WITH BIDIRECTIONAL DATA" procedure;

Figure 9 illustrates an example of a "BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA" procedure;

Figures 10A, 10B and 10C are flow diagrams showing examples of processes by which the server maintains a connection with the client and communicates commands and data to it.

Detailed Description of the Invention

In the above description, the invention is described using various embodiments of the present invention as examples but the invention is not intended to be restricted to these embodiments. It is understood that other embodiments may be utilized and structural and operational changes may be made without departing from the scope of the present invention.

Figure 4 illustrates an exemplary implementation of the system for pushing application commands to a mobile terminal based on server side and client side events in accordance with one embodiment of the present invention. More specifically, Figure 4 illustrates a Push Client basic functionality 405 implemented in a mobile terminal 404 as part of a message passing system in cooperation with a Push Server 401. The push client 405 is preferably implemented in the form of a software run in a processor of the mobile terminal 404. The mobile terminal 404 is preferably a commercially available mobile terminal, such as a portable phone or appliance capable of running software or personal digital assistant, which provides a platform for downloading application software over air or from a personal computer, installing the software in the terminal, and running the software in the terminal. For example, the Symbian operating system is an open operating system, application framework, and application suite optimised for the needs of wireless information devices such as intelligent phones, smartphones and communicators, and open operating system and drives standards for the interoperation of data-enabled mobile phones with mobile networks, content applications, and services. The Symbian operating system also includes connectivity software for synchronisation with data on personal computers and servers. The application may be in an appropriate programming language, such as C++ or Java, which is an object-oriented pro-

gramming language and virtual machine platform developed by Sun Microsystems.

The push client software 405 preferably launches automatically when the mobile terminal 404 is turned on. The push client software 405 runs in the background and attempts to log into the push server 401 over a data network 403, normally a wireless network capable of transmitting Internet Protocol (IP) packets. The arrow A in Figure 4 illustrates an optional attempt by the push client 405 to communicate with the wireless network firewall 402 or other similar security or gateway device in order to open a connection for the push server 401 to directly contact the push client 401 as in FIG 3. If successful, operations can continue as described in FIG 3 or as below. Arrow B illustrates a login attempt.

The wireless network 403 may be protected by means of a firewall or other appropriate security entity 402, which connects the wireless network to the public networks and filters and selectively discards the data packets entering and exiting the wireless network according to predefined rules. Thus, a firewall is a gateway device which operates at the same time as a connector and a separator between networks in a sense that it keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Additionally, IP connection techniques, such as Internet Protocol 4 (IP4) network address translation and Internet Protocol 6 (IP6) security, encryption and/or authentication, may hide the actual address of the mobile terminal or make it otherwise difficult for a server to connect to directly to the mobile terminal. The public telecommunications operator, company, organization, or private individual setting up this mobile Internet space with one or more users having greater ability to contact one another and included servers does this to protect the mobile terminals from hostile or unwanted contact common on the public Internet. They may also do so to reduce background traffic, protect their control over this space and limit outside or undesired service providers through technical connection policies set in the firewall, gateway or other security device. Physically a firewall may be a machine with appropriate software to do the task assigned to it. 402 can be a firewall, router, a personal computer, a gateway server or whatever similar computing device, infrastructure or secure protocol such as IP6 can be used for such purposes.

Consequently to the existence and configuration of 402, if a fixed or mobile computing device from outside the controlled mobile network tries to contact a mobile terminal 404 inside the controlled mobile network, the incoming connection is not generally permitted unless the organization or individual controlling the firewall, gateway server or security device 24 makes an adjustment to their security policy and explicitly allows the connection.

From point of view of the wireless packet data network 23, the login attempt B and associated connection establishment C is one or more normal IP connections established at the request of the mobile terminal. If optional attempt A to open a path for the push server 401 to initiate the IP connection now or in the future, use from that point forward may proceed as in FIG 3. However this firewall and/or security device or protocol opening A is unsuccessful, the login attempt B is in either case normally allowed to pass the firewall or security infrastructure 402 since the connection is from the inside the firewall to outside.

After attempting login, if the login is not successful the client 405 may automatically or under supervision of the user of the mobile terminal 404 try several different techniques for contacting the server 401. Since there are numerous variations between mobile terminals and in network connectivity, more than one connection attempt may be needed to contact the push server 401. Differences in wireless network terminal characteristics, individual push server availability and accessibility, firewall and gateway permissions, connection timeouts, connection level stateful (such as TCP) and stateless (such as UDP) transport protocol availability (such as IP4, IP6, SSL, HTTP, HTTPS) and alternate mobile terminal network settings mean that a sequence of connection establishment attempts and connection maintaining steps may required to be made using variations in relevant network parameters.

A second reason for automatically adjusting the network parameters is not simply establishing the connection but establishing the connection in the most cost effective or highest performance configuration available for the individual mobile terminal user account service level. Connection types differ in speed, customer expensive, server resource usage and hence scalability, security and ability to penetrate gateway security devices. Some customers may be offered more secure or higher performance service while others receive the least cost connectivity from either the mobile terminal's or the push server's standpoint.

As an example, such network parameters may include but are not limited to one or more of the following:

- Use of a connection-oriented protocol suitable to the wireless network such as TCP/IP protocol, which is generally preferred in the common situation where an intermediate firewall, Network Address Translation (NAT) or gateway device 402.

- Use of a connectionless protocol suitable to the wireless network 403, such as UDP/IP, which is generally preferred when no network device restricting terminal contact 402 is present as this reduces resource usage on the server when large number of mobile terminals is served.

- Use of an alternate connection-oriented protocol such as HTTP suitable for mobile push operation through more strict firewalls and proxy Internet connections.

- Use of a secure protocol such as HTTPS, IP-Sec, secure IP6 or a proprietary security protocol to identify the communicating parties, prevent message interception by 3rd parties, and prevent message modification by 3rd parties.

- Use of a periodic message from the client to the server or server to the client to the effect that client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices do not time expire the connection.

- Use of configuration messages to the firewall (FIG 4, A) using a firewall or other security configuration protocol, such as Universal Plug and Play, to open a path for server-initiated connection-oriented or connectionless messaging to the client.

- Use of periodic messages initiated by the client 405 or by the server 401 to the effect that the receiving application is informed that their messages are continuing to be received, as indicated by response data from the receiving party to the sending party.

- Use of longer or shorter timing between such periodic messages to match the combined needs of all such network devices and protocols involved in transmitting communication, as adjusted based on the success or failure of earlier messages to successfully traverse the open network connection.

- Use of an alternate push server network address such as an address accessible with fewer security and performance restrictions which may be more available, more accessible, lower cost, lower latency, less busy, higher

bandwidth or otherwise preferred at the present time and from the present network location of mobile terminal 404.

- Use of one or more alternative mobile terminal network connection settings, or variation of the parameters within the settings.

- Use of an alternate connection route through a second mobile or fixed terminal accessible to the mobile terminal over an alternate wireless network or network connection and capable of communication with a push server.

In an embodiment of the invention, the mobile terminal 404 keeps a prioritized data structure listing the preferred communication protocols, server addresses, periodic message timings, network access settings, and alternate communication routes which it should use. Automated and manually assisted use of this structure should then result in a connection to one or more push servers, however if one of these connections which the mobile terminal is programmed to expect is not available, the mobile terminal can choose the sleep that function of the client software and attempt re-connection at a later time, repeating in like fashion with the same or different network connection parameters as described above until a connection is established or other user intervention.

At any time after a connection is established between the client 405 and the server 401, the client may push a message to the server or the server may send a push message to the client. This is illustrated by means of the arrow C in Figure 4. These messages through a previously established, connection-oriented protocol such as TCP/IP, SSL, HTTP or HTTPS arrive quite rapidly, more rapidly than if the connection were established only when needed. The associated protocol overhead such as 3-way handshake during connection establishment thus occurs before the actual need for message transmission rather than needing to occur at time of transmission and thus delaying the transmission.

A connectionless protocol, such as UDP/IP, may also be used in cases where the connection-oriented protocol is not possible or not desirable because of the push server resources used by every static instance of a connection-oriented protocol. Connectionless communication is also used when a message needs to get through to the server 401 quickly, such as when occurs when the client 405 notifies the server 401 of a terminal event, user interface event or application event but the connection-oriented protocol connection is not connected or is already busy transferring information. Such a selective use

of this high priority, low latency communication channel from terminal 404 to server 401 gives the server the opportunity to in return push to the client 405 a service triggered by the event begin communicated by the client 405 as will be described in more detail below. The sending of such a return message is frequently time critical and the fastest available combination of techniques will be used.

In the preferred embodiment of the invention, the most basic message pushed from the server 401 to the client 405 is a data packet containing no information. Additional binary or text information specifying which mobile application 406 from a plurality of such applications may optionally be included. Additional binary or text information to be passed to the default or specified mobile application may optionally be included. Additional binary or text information specifying how upon receiving such a message the client 405 will notify and optionally ask the user if the action should be performed may optionally be included. Upon receiving such a message, appropriate automated actions and user interface media capabilities of the mobile terminal as specified in the command C from the server 401 are executed by the push client 405. The most common case is playing a sound, asking the user if the mobile application should be launched, and if affirmative passing the command details (arrow D) to the specified mobile application, module or additional feature within the same application suite, launching the application, module or feature if needed. Such action may include optionally proceed without audio, with network downloaded audio, or without first requesting confirmation from the user as specified by user preferences and command details.

The push message from the push server 401 may be triggered by any trigger event, local or remote, defined at the server. The trigger may, among others, include an alarm, notification, or measurement result received to the push server 401 from another device or system. With a push message, the server 401 may direct the mobile application 406 to make use of additional network resources either on the push server or other server. The push client 405 may in turn at any time accept data D from each of a plurality of mobile applications 406 and direct such to the push server 401, possibly for redirection through push server API to other servers, mobile terminals, push clients and computing devices.

Figure 7 illustrates an example of an "COMMAND PUSH" procedure wherein the push server 701 is triggered by a trigger event as for example from

an application server 702 to push an application command message to the push client 704 and thereby initiate a mobile terminal client trigger event in a mobile application 705 from a plurality of such applications, program modules and user interface features on the terminal 705. The trigger event from push client 704 to mobile application 705 may optionally include commands or data affecting the aspect of visual presentation of mobile application 705. The even trigger mechanism may be any electronic process mechanism as for example computer software calls to load or configure a class, library, dynamic link library, MIDlet, Symbian application, Linux daemon or other executable object. The trigger mechanism may be between separate parts of a larger application or application suite, or may be an IP-triggered application launch and data transfer as in the case of mobile application launched by contact to a specified IP port. The potential applications of the COMMAND PUSH include but are not limited to mobile applications for enterprise connectivity, back office integration, database access, scientific and industrial process and equipment monitoring and control, pictures transfer, mobile gaming, application data transfer, mobile electronic commerce, application alarms, reminders, multimedia interactivity, corporate calendaring, personal messaging and group messaging, etc.

The push server 701 may in combination with user preferences stored in either the push server 701 or push client 704, optionally request the push client 704 to display or otherwise as appropriate for the mobile terminal or appliance notify the user asking permission for launching mobile application 705 prior to application launch. The preferred embodiment is for the behavior, language and content of this information to be configured on the server 701 based on the service and preferences of the individual receiving the message. In such cases an optional informational message will be presented to the user and such information messages are associated for instance with the menu option transmitted to the client 704 by the server 701.

In an embodiment of the invention, the client 704 is also capable of receiving and storing variables which configure behavior of the client 704. The server 701 may thus specify the network connection preferences, notification sounds, and other behavior of the client 704. These changes facilitate the efficient and manageable operation of the entire system and can be used for automated remote maintenance of push client 704, mobile applications as 705, and configurable aspects of underlying mobile terminal 703, for example

changing the username, password, and security certificates stored in the mobile terminal.

Figure 8 illustrates an extension of the procedure in Figure 7, one known as "COMMAND PUSH WITH BIDIRECTIONAL DATA". This embodiment of the invention includes all aspects of "COMMAND PUSH" with the additional step that a data connection between application server 802 and mobile application 805 is established with the aid of the persistent managed, tested and configured data connection in Figure 4, arrow C between push server 401/801 and push client 405/804. An IP or other API (application programming interface) connection between application server 802 and push server 801 simplifies the work and cost of creating application server 802 by taking care of network details already established for the COMMAND PUSH procedure. Similarly, an IP or API connection between push client 804 and mobile application 805 completes the connection and reduces the number, cost and resource usage of a possible plurality of such connections for a corresponding plurality of mobile applications. Further, each mobile application 805 is now free to sleep, exit or otherwise release the limited resources of the mobile terminal 803 with the assurance it may be remotely commanded back into action provided at least one push client 804 from a possible plurality of such push clients remains active, connected to the push server 801 and configured to launch the mobile applications 805.

Referring now to Figure 5, users of mobile terminals 507 are frequently but not continuously in range of alternative and more desirable wireless network access (Figure 5, arrow A). Such access is shown in the exemplary embodiment as broadband access point 509 within alternate and more desirable for reasons such as speed, cost and security broadband wireless network 507. Such an access point 509, which may also be mobile, is referred to herein as a broadband access terminal. The push client network connection functionality according to the invention may also be installed on such a broadband access point to facilitate routing and connection over alternative wireless network 507 such as a bluetooth, Wi-Fi, Wi-Max, Zigbee, radio frequency, infrared, ultrawideband, grid network or similar opportunistic or ad-hoc wireless network. Thus, both devices 508 and 509 have the minimal capabilities of client software 405 necessary for establishing and maintaining the already established contact with push server 501. Further, the two devices detect one another and so noting inform the server 501 through connections B or C and are thereafter

temporarily associated with one another in the server for routing and mobile application launch and data transfer purposes. Further, the push server 501 on becoming aware of such a situation may inform (arrow D) the application server 502 of the availability of a more desirable network connection (C plus A) to the client and on behalf of the application server 502 or independently decide to push additional commands and data to the wireless terminal using this connection. Further, the push client in the broadband access point has the additional capability to route such information to the wireless terminal. The result benefits customers using the wireless terminal in that data is managed and updated automatically for their mobile applications in the most cost efficient manner for non-time-critical capabilities such as lazy application code update and lazy application data update. While such alternative routing may also be achieved through normal IP routing and path cost without the presence in the broadband access point 509 of push-aware client software, the push server 501 and application server 502 would in this known-in-the-art implementation not be aware of when the low cost alternative route was available and thus able to at such time trigger the push of lazy application code and data installation and updates.

Figure 9 illustrates an example of a "BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA" extending the earlier discussed "COMMAND PUSH WITH BIDIRECTIONAL DATA" disclosed in Figure 8. This procedure wherein the push server 901 has been earlier informed by either the mobile terminal push client 906 or broadband access point 904 of the available alternative broadband network 507 and associated route (Figure 5 D, C and A, corresponding to Figure 9 A, B and C). Based on this notification and user preferences the push server 901 may choose to route future messages to either device, however the preferred remote application command push and data route is indicated by arrows B and C. Then at some later time the push server 901 is triggered by a trigger event of which the application server 902 is aware to send push message to the mobile terminal 905, and procedure steps A, B, C are traversed thereby pushing application launch commands, lazy application updates, and lazy application data updates through push clients 904 and 905 to mobile application 907 through local command and data path D (also Figure 5, arrow A).

Figures 6A, 6B, 6C and 6D are flow diagrams showing examples of processes of the preferred embodiment by which the client 405 maintains a connection with the server 401 and communicates messages to it.

Firstly, in step 602 the push client 405 initiates an attempts to log into the push server 401 over data network 403, as indicated by the arrow B in Figure 4. Success of the connection attempt is monitored in step 603, and if the network connection shows an error or does not get a response from the server in a reasonably short time the network settings are adjusted in 604 (for example in the manner describe above if the network connection fails). If the server does connect but login fails at 605, the push client may change the login settings in step 606 (for example in the manner described above if the login is rejected) and retry the login. If the login to the push server 401 is successful, a connection is already opened to the client 405 and the application server 405 changes state informing applications server 502 from a plurality of such server of the availability of the client 401 and relevant details. Thereafter the mobile applications 406 of a plurality of such applications can be contacted until the server 401 is otherwise notified or decides based on exceptions in network communications that the terminal 404 has disconnected.

In association with the login procedure the client 405 may attempt to communicate with the mobile network firewall, gateway or security device 402 it is behind using a firewall configuration interface, such as the Universal Plug and Play (UPnP) Internet gateway configuration protocol (the arrow A in Figure 4). In an alternative embodiment t may do so either before step 601. In either case the client 405 requests the firewall 402 to open an IP hole allowing the server 401 to initiate contact with the client 405 whenever there is need a need thereafter allowing classic prior art mobile application launch as illustrated and described in Figure 3. In the preferred embodiment, the configuration of the firewall 401 to allow incoming messages in this manner is attempted in step 607 immediately after login, and if the security opening operation appears successful (step 608) the server 401 is notified by the client 405. The server 401 then attempts this type of direct IP connection to the client 405 or mobile application 406 (step 609), and if that too is successful (step 610), then one of these test connections is closed and both server 401 and the client 405 mark the second connection as closable (step 611) since they now know that they may save bandwidth charges and resources by closing the connection knowing that server 401 has now gained the ability reopen the connection when

needed for a classic command push procedure (Figure 3, arrow A) or other data communication use. At any time after this point the server 401 or the client 405 may choose to close the remaining network-level connection (usually a TCP or SSL connection) while keeping the application-level "connection" in the form of knowledge of how the server 401 can contact the client 210. The advantage of such an application-level connection without the network-level connection is lower use of network resources particularly on the server side thus significantly increasing server scalability for infrequent command and data push applications by decreasing overhead cost per active user.

Referring to steps 620 and 621 in Figure 6B, after the login and connection setup in Figure 6A, the push client 405 may send a periodic message (the arrow C in Figure 4) from the client 405 to the server 401 to the effect that client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices do not time expire the connection. The period of time (measured in seconds, minutes or hours and varying from mobile network to mobile network) between such periodic messages is set to match the combined needs of all such network devices and network protocols involved in transmitting communication (step 604). The client 405 may then wait for a reply or acknowledgement from the server 401, and if the acknowledgement is received (step 622), the client 405 returns to step 620 to await the next combined connection refresh and test. If the no acknowledgement is received, the client 405 may return to step 604 in Figure 6A to possibly automatically adjust network settings or, if it deems the settings correct but the network not available, simply re-attempt login to the server 401.

Referring to Figure 6C, after the login and connection setup, the push client 405 is ready to receive the push messages over the connection from the server outside the operator's firewall (step 631). If a push message is received, the client 405 executes the corresponding function, such as launch or pass commands and data a mobile application (step 632). If required, the client 405 may also send a message to the server 401 (step 633), such as a command execution acknowledgement or result.

Referring to Figure 6D, after the login and connection setup, the push client 405 may monitor the local resources for a state change (a trigger event) in step 641. If a state change of other event is detected in step 642, the push client 405 may send a message to the server 401 (step 643).

The push server 401 can be server software run on any appropriate computing device. Figures 10A, 10B and 10C are flow diagrams showing examples of processes by which the server 401 maintains a connection with the client 405 and communicates push commands and other data to it.

In step 1001 of Figure 10A, the push server 401 receives a login from the client 405 initiates an attempt to log into the push server 401 over a packet switched network 403, as indicated by the arrow B in Figure 4. In step 1002, a connection is opened to the server 401 and the server 401 is informed of the client's its availability and the details by which the client 405 can be contacted until the server 401 is otherwise notified or detects a network fault or shut-down. In step 1003, the server 401 attempts this type of classic IP push connection to the client 405, and if that is successful (step 1004), then one of these connections is closed and both the server 401 and the client 405 mark the second connection as closable (step 1005).

Referring to steps 1010 and 1011 in Figure 10B, after the login and connection setup, the push server 401 may receive a periodic message (the arrow C in Figure 4) from the client 405 to the effect that the server updates the respective server object associated with a given client so that the connection, server socket or client socket is not time expired as being stale. The server 401 may send a reply or acknowledgement in step 1012 to notify client 405 of successful network, firewall and security traversal.

Referring to step 1021 Figure 10C, after the login and connection setup, the push server 401 monitors for trigger events and event messages. If the server 401 is triggered by a trigger event (the result "yes" in step 1023), it decides based on application-specific logic and/or user preferences whether the resulting push procedure is a BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA procedure in step 1024. In case of BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA, the server 401 sends the command or data push message to the push client 508 through the push client 509 (step 1025). If not using this alternative network connection selected in step 1024, the push server 401 proceeds to step 1026 to perform a more classic COMMAND PUSH or COMMAND PUSH WITH BIDIRECTIONAL DATA. In case of COMMMAND PUSH, the server 401 sends an command push message to the push client 405 and thereby forces a mobile application 406 from a plurality of such push-aware mobile applications in the mobile terminal as specified in the command (step 1026). In the case of COMMAND PUSH WITH

BIDIRECTIONAL DATA, the push server 401 sends the client 405 push commands or data and may return response through the same IP connection (step 1026).

If the server 401 is not triggered by a trigger event (the result "no" in step 1022), it checks whether an event message has been received from the client 405 (step 1023). If not, the process returns to step 1021. If an event message has been received from the client 405, the server checks whether a proximity detection is involved indicating that the mobile terminal 508 can connect to a broadband access point 509 (step 1024). If the broadband access point 509 is connectable, the server 501 performs accordingly, typically by sending an command or data push directly through the broadband access point in a manner described with reference to Figures 5 and 10C (step 1025). If the alternate broadband connection is not available or not preferred in preferences, the server delivers the message directly as above (step 1026).

The above specification, examples and data provide a complete description of the manufacture and use of the system, method, and article of manufacture, i.e., computer program product, of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

Claims

1. A method of pushing commands and data to a wireless terminal from a push server located outside a wireless system serving the wireless terminal, comprising

the push client initiates and maintains over an extended period of time a packet-based data connection through at least one communication security or inter-network connection device of the serving wireless system to the push server using Internet technologies;

the push server sends, in response to predetermined trigger events, at any time push application installation, updates, commands or data messages to be directed to a push application or dynamically loaded module or user interface feature from among a plurality of such applications, modules and features by means of said client-initiated or client-opened and client-maintained permanent connection, whereby avoiding blocking of said server-originated push messages by the security device, and launching said application, application module or dynamically loaded module or user interface feature as needed,

the push client, in response to receiving a push message containing application installation, updates, application commands or data from the push server, forwards such application commands or data or stores such application installation or updates within the mobile terminal to a mobile application from among a plurality of such applications so as to initiate launch optionally to a specified state or if already running initiate or change presentation to the user according to the push message.

2. A method as claimed in claim 1, comprising

the push client sends configuration messages of a security device configuration protocol to the security device to open a path for later server-initiated connection-oriented or connectionless messaging to the push client.

3. A method as claimed in claim 1 or 2, comprising

the security device is a security protocol such as IPsec whereby the client may open the possibility for the server to contact it by exchanging security keys or otherwise enabling subsequent server-initiated contact.

4. A method as claimed in claim 1, 2 or 3, comprising

the push server attempts server-initiated messaging through the security device to the push client after having being informed of the client-initiated connection.

5. A method as claimed in claim 1, 2, 3 or 4, comprising

the push server and the push client after testing the ability of the server to open a connection to the client mark the maintained network-level connection closeable,

the push server and the push client can close said network-level connection while keeping an application level connection information indicating future possibility for the push sever to reopen said network-level connection when needed.

6. A method as claimed in any one of claims 1-5, wherein the step of maintaining further comprises that the push client maintains the permanent connection through the security device by sending periodic keep-alive messages.

7. A method as claimed in any one of claims 1-6, comprising the push client or the push server sends a periodic reply to messages initiated by the push server or by the push client, respectively, to the effect that the receiving end is informed that the messages are continuing to be received.

the push client or the push server upon failure to receive acknowledgement of said periodic reply may choose to open a new connection.

8. A method as claimed in claim 6 or 7, comprising use of varying timing between the periodic keep-alive or reply messages to match the combined needs of various network devices involved in transmitting and maintaining communication.

9. A method as claimed in any one of claims 1-8, comprising if an attempt to contact the push server during initiation of the permanent connection and login is not successful, the push client automatically or under supervision of the user of the wireless terminal tries one or more other techniques, protocols and/or network parameters for contacting the push server.

10. A method as claimed in claim 9, wherein said trying of one or more other techniques and/network parameters include one or more of

using an alternate push server network address which may be more available or more accessible at the present time and from the present location,

using one or more alternative mobile terminal network connection settings, or variation of the parameters within the settings,

using an alternate connection route through a second wireless or fixed terminal accessible to the wireless terminal over a wireless network and capable of communication with the push server,

using a TCP connection,
using a UDP connection,
using an SSL connection,
using an HTTP or tunneling HTTP connection,
using an SHTTP or tunneling HTTPS connection,
using an XML-based connection over other transport protocol.

11. A method as claimed in any one of claims 1-10, comprising the push client stores in the wireless terminal a prioritized data structure listing preferred communication protocols, server addresses, periodic message timings, network access settings, and/or alternate servers and communication routes and uses this data structure to attempt reconnection to the push server if the connection to the server fails.

12. A method as claimed in any one of claims 1-11, wherein the connected networks on which the push server and mobile terminal are located are private networks which allow greater interconnectivity than they both offer to the public Internet.

13. A method as claimed in any one of claims 1-12, wherein the message the push server sends to the push client includes an application launch or reconfiguration push message directing the immediate or subsequent actions and data of the application.

14. A method as claimed in any one of claims 1-13, wherein the push server sends to the push client include an application command or data or reconfiguration message redelivered by the push client as an API call or IP connection between processes running on the same mobile terminal.

15. A method as claimed in any one of claims 1-13, wherein the push server sends to the push client is new application code, application code updates or application data updates.

16. A method as claimed in claim 13-15, wherein the push client is a library or process installed independently or together with but containing or enabling the functionality to supply push messages to one or more of a plurality of applications, modules or dynamically loaded module or user interface features on the mobile terminal.

17. A method as claimed in claim 16 wherein only one of the possible plurality of push clients need operate at a given time, providing push services for a plurality of push-aware applications on the mobile terminal.

18. A method as claimed in any one of claims 1-17, wherein the message the push server sends to the push client includes an optional application launch or event push message triggering the wireless terminal to play a sound notifying the recipient of the message and/or to display notification information such as text, rich text, graphics and rich media from which the user may select or decline to launch the application, dynamically loaded program module or user interface feature based on push message or messages recently received.

19. A method as claimed in 18, wherein the notification sound, text, rich text, graphics and rich media presented by the terminal is selected by and deliverable from the server and may be retrieved from the server by the terminal, thereby allowing the push server to indicate through audio and media signals including note sequences, audio samples sound modification applied to note sequences and audio samples, spoken speech, color, motion, shape and design the message sender, nature, priority, content and other attributes of the received message, message sender and/or message sender current state.

20. A method as claimed in 19, wherein the specified notification information and media is played from a cache in the terminal and the cache is automatically updated over the air as needed with new notification information and media.

21. A method as claimed in any one of claims 1-20, wherein said trigger events include events which the push server is aware of and/or events which the push client is aware of and which a push client from among a plurality of such push clients makes the push server aware of.

22. A method as claimed in any one of claims 1-21, wherein said trigger events include one or more of: the making, receiving, and termination of telephone calls, the transition from presence-to-absence or absence-to-presence of other devices in a physical contact, RF, near field, infrared, personal area, local area, metropolitan area or geographical area wireless communications network, an alarm, notification, videogame action or event, remote application user or application server event, remote user action or inaction, electronic or computing equipment change of state or measurement result.

23. A method as claimed in any one of claims 1-22, comprising the push client in the wireless terminal detects availability of an alternate wireless network connection to a broadband access terminal, or the broadband access terminal detects ability to initiate contact to the wireless terminal,

the push client is responsive to receipt of command and data, application installation and update push messages through said broadband access terminal.

24. A method as claimed in any one of claims 1-23, comprising

the push client in the wireless terminal detects network connection availability of a terminal device with a higher bandwidth capacity or otherwise specified as preferred, or the device with a higher bandwidth capacity detects such ability to connect to the wireless terminal

the push client transmits connection availability information of the higher bandwidth device to the push server, or the large bandwidth terminal transmits connection availability information of the mobile terminal to the push server,

the push server uses the connection availability information as a trigger event for sending lazy or low priority messages including application updates and application data updates routed through the higher bandwidth capacity device to the wireless terminal.

25. A method as claimed in any one of claims 1-24, comprising

the push client in the wireless terminal detects connection availability of a higher bandwidth or more desirable alternate network connection device,

the push client transmits connection availability information of the higher bandwidth device to the push server,

the push server uses the connection availability information as a trigger event for routing messages directed to the user of the wireless terminal through the higher capacity device.

26. A method as claimed in claim 25, comprising

the push server stops directing messages to the higher capacity device when the wireless terminal is no longer connectable to the higher capacity or more desirable alternate wireless network connection device.

27. A method as claimed in any one of claims 24-26, comprising

providing the higher network connectivity device with a push client with server connectivity similar to that in the wireless terminal.

28. A method as claimed in any one of claims 1-27, comprising

the push client in the wireless terminal detects connection availability of a device with a better alternative network connection, or a push client in the device with a better alternative network connection detects connection availability of the wireless terminal,

establishing a data-transfer capability between the push clients,
routing communication to and from the push client in the wireless terminal through the push client and the network connection of the better alternative network connection device.

29. method as claimed in any one of claims 1-28, comprising
customizing the appearance, notification sound or look and feel of the messages received to based on message source, message source state, message parameters or message recipient preferences.

30. A method of pushing messages to a wireless terminal from a push server, comprising

the push server sends, in response to predetermined trigger events, at any time application push messages to a push client in the mobile terminal,

the push client in the wireless terminal detects connection availability of a device with a preferable alternative network connection, or the device with a preferable connection detects connection availability of the wireless terminal,

the push client is responsive to receipt of the application push message to push commands to an application in said device with a larger screen so as to bring forward view an application view identified by, modified by, contained in or otherwise affected in presentation by the received application push message.

31. A method of routing messages to a wireless terminal from a push server, comprising

the push server sends, in response to predetermined trigger events, at any time application push messages to a push client in the mobile terminal,

a push client in the wireless terminal detects a device with a preferred alternative network connection, or a push client in the device with a network connection detects physical proximity of the wireless terminal,

establishing a data-transfer capability between the push clients,

routing communication to and from the push client in the wireless terminal through the push client and the network connection of the device.

32. A method as claimed in any one of claims 1-31 wherein the push client accepts compressed information and optionally decompresses such information for the mobile application.

33. A method as claimed in any one of claims 1-32, wherein the push client and push server establish a secure connection and unwrap such security on behalf of the mobile application.

34. A server comprising means for performing the server steps as claimed in any one of method claims 1-33.

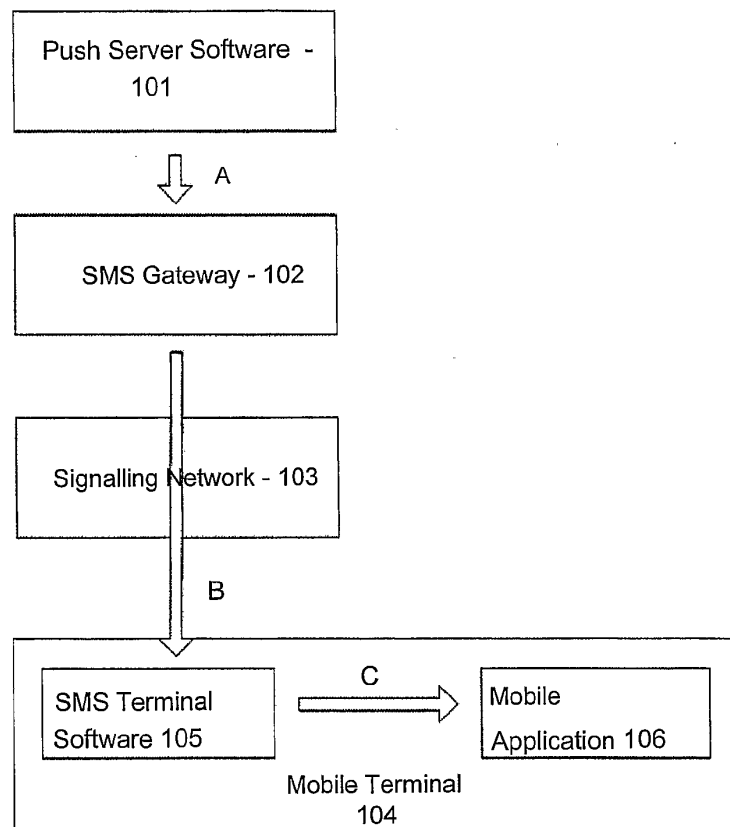
35. A wireless terminal comprising means for performing the push client steps as claimed in any one of method claims 1-34.

36. A program product comprising program code means which, when run in a computing unit of a wireless terminal, performs the push client steps as claimed in any one of method claims 1-35.

37. A program product comprising program code means which, when run in a computing device, performs the push server steps as claimed in any one of method claims 1-37.

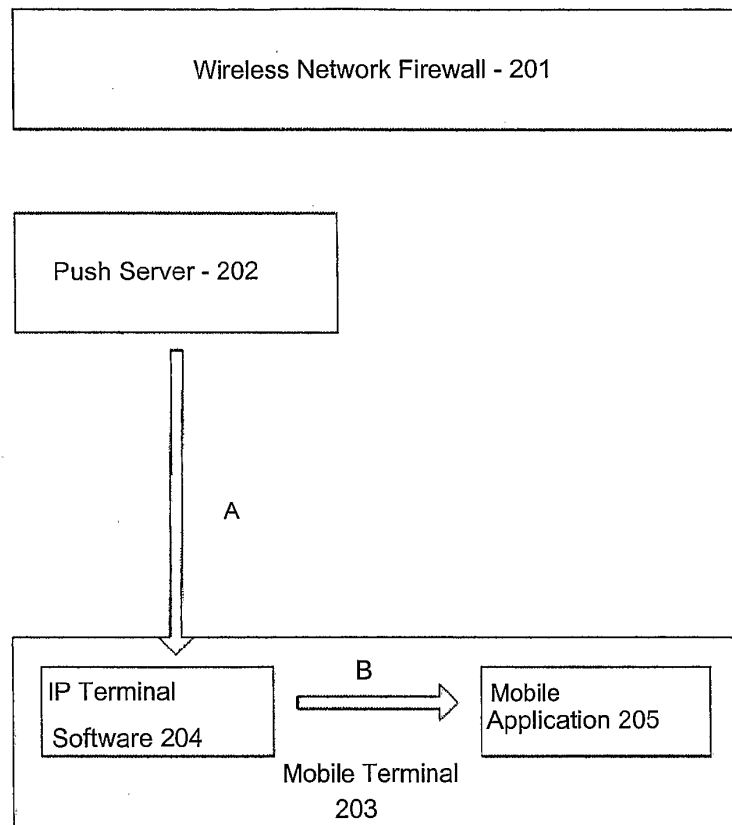
1/15

Figure 1



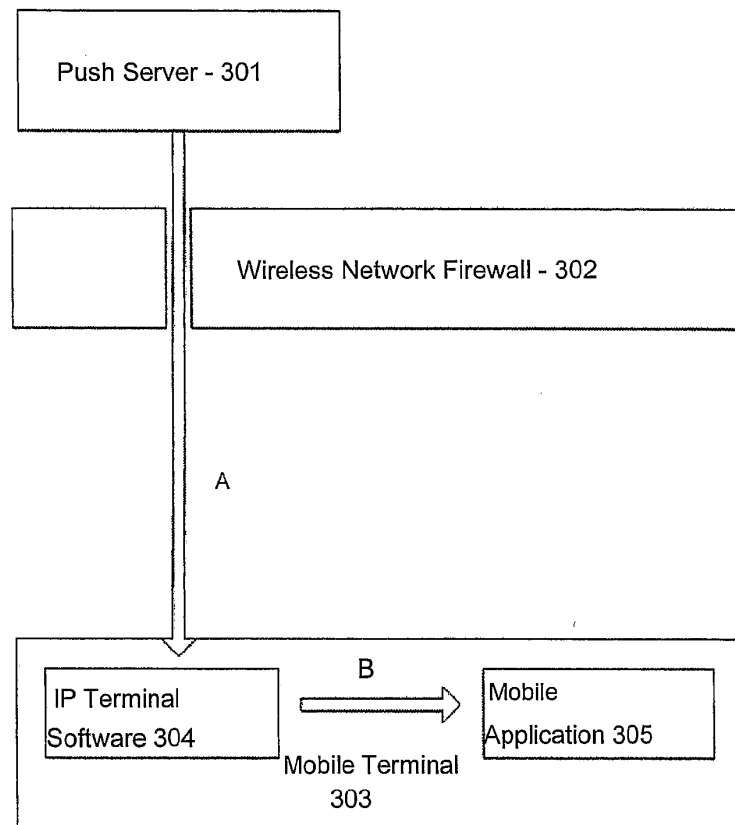
2/15

Figure 2



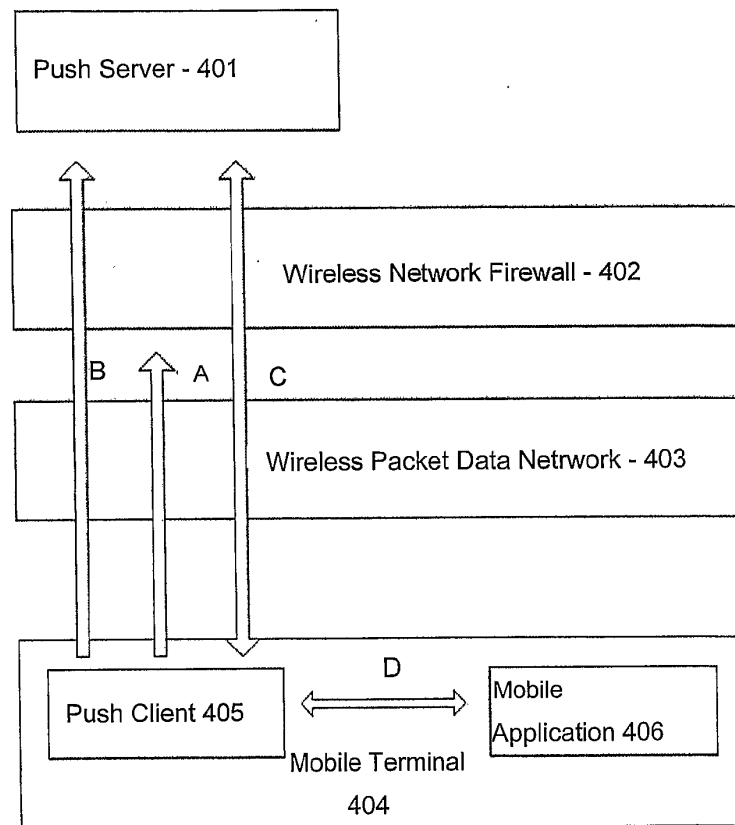
3/15

Figure 3



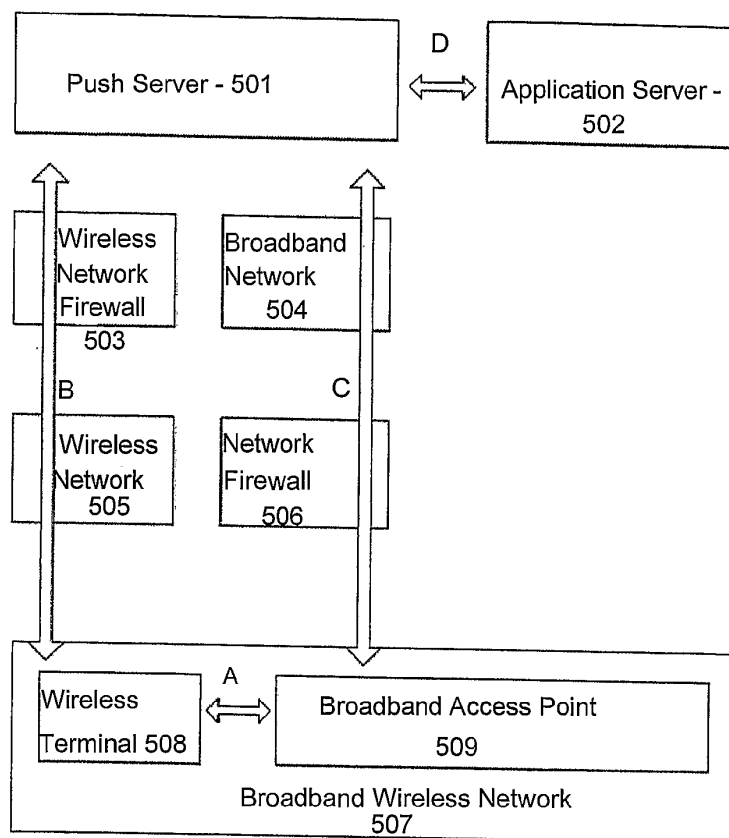
4/15

Figure 4



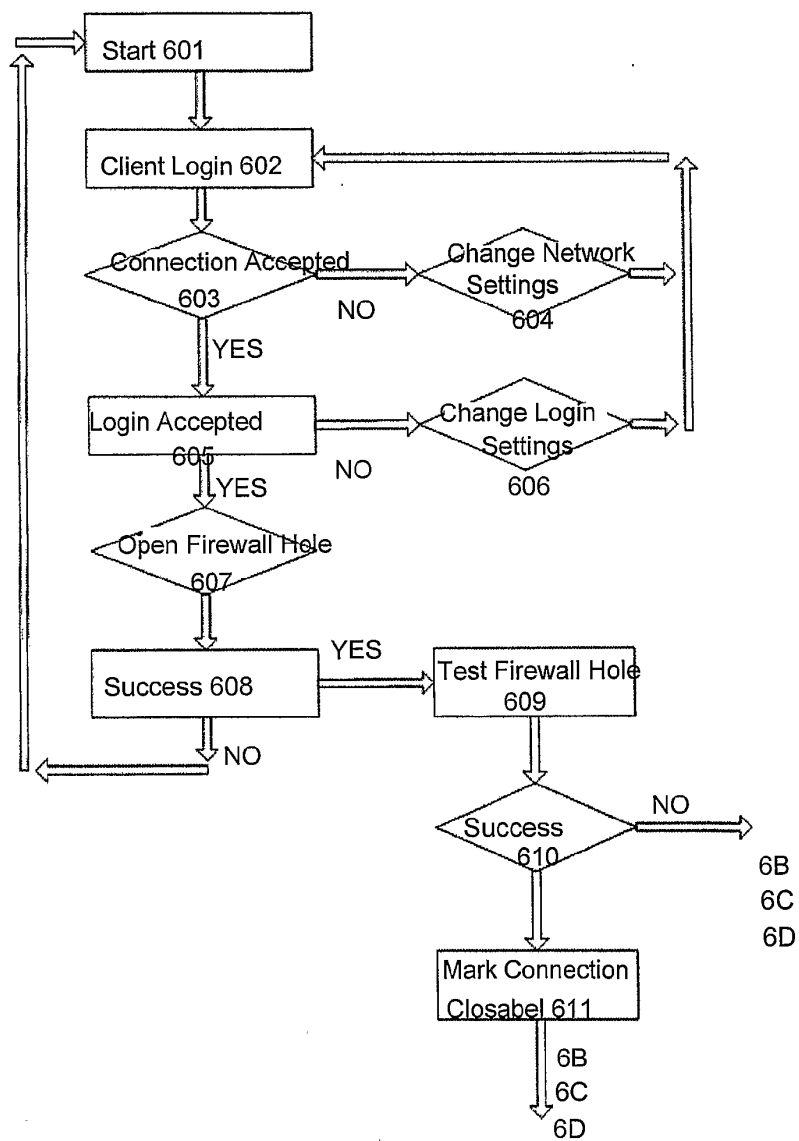
5/15

Figure 5



6/15

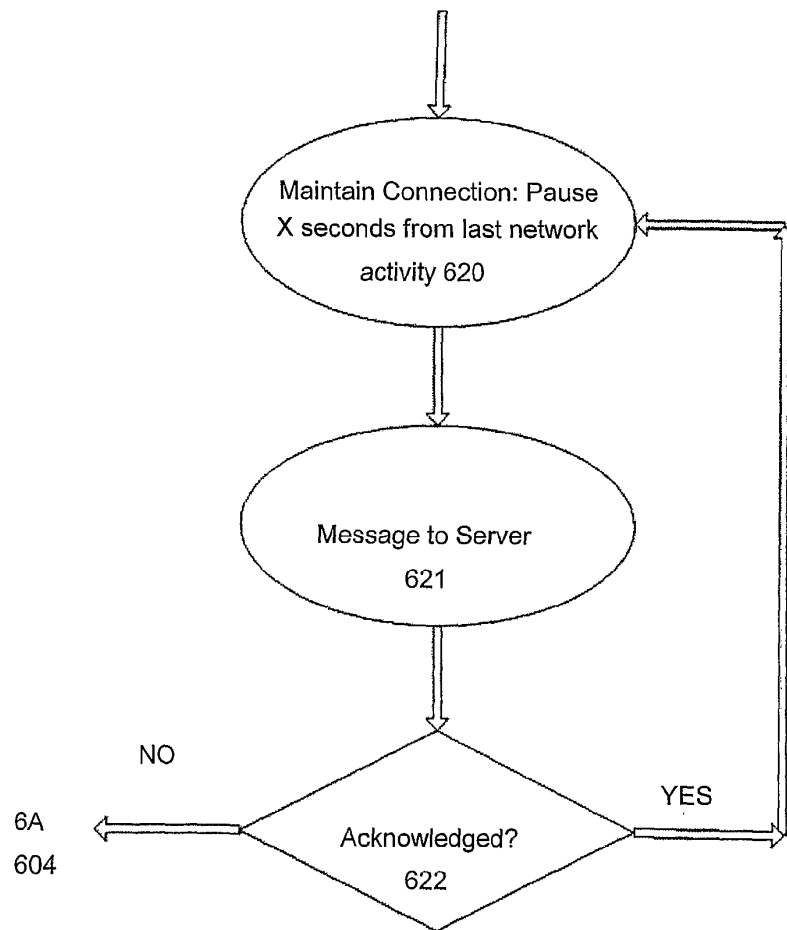
Figure 6A



SUBSTITUTE SHEET (RULE 26)

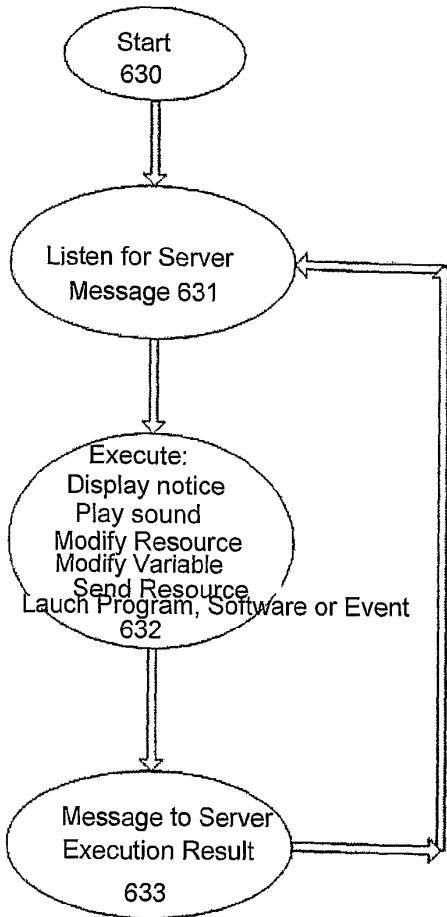
7/15

Figure 6B



8/15

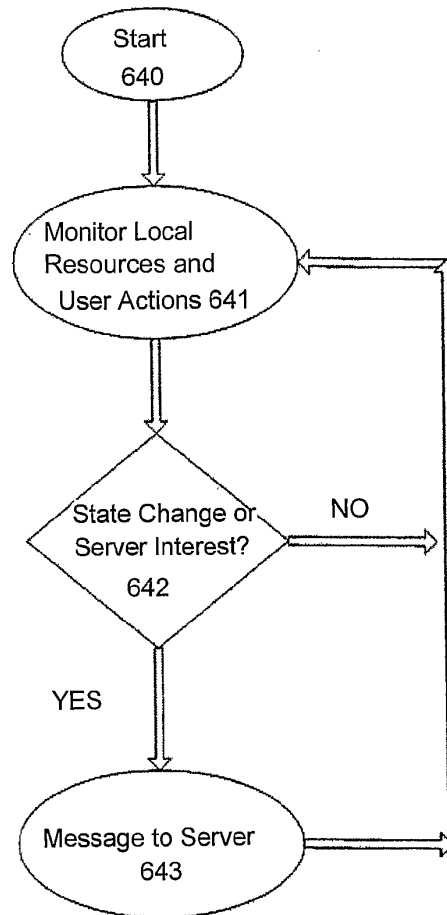
Figure 6C



SUBSTITUTE SHEET (RULE 26)

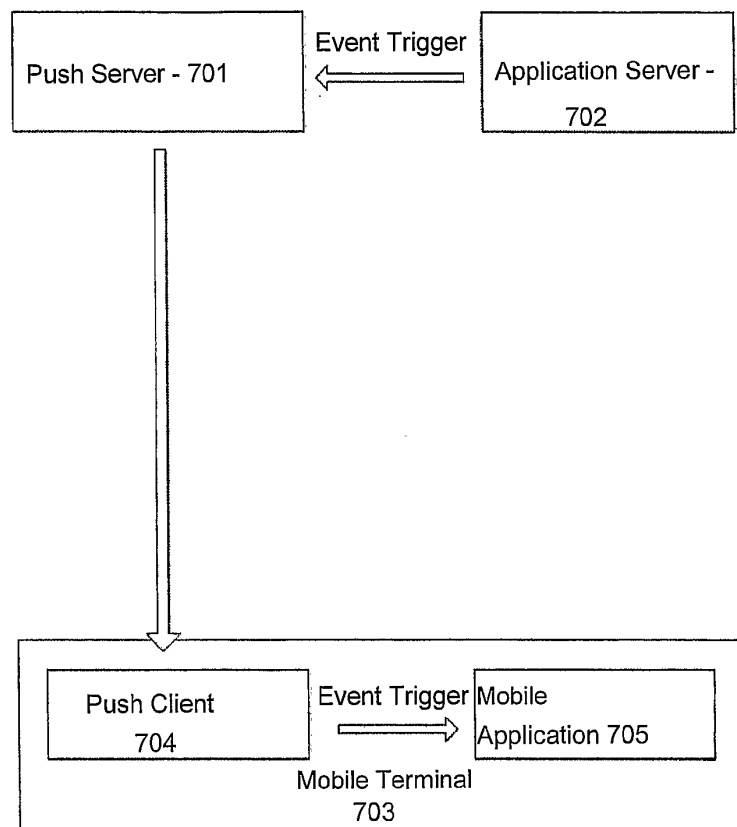
9/15

Figure 6D



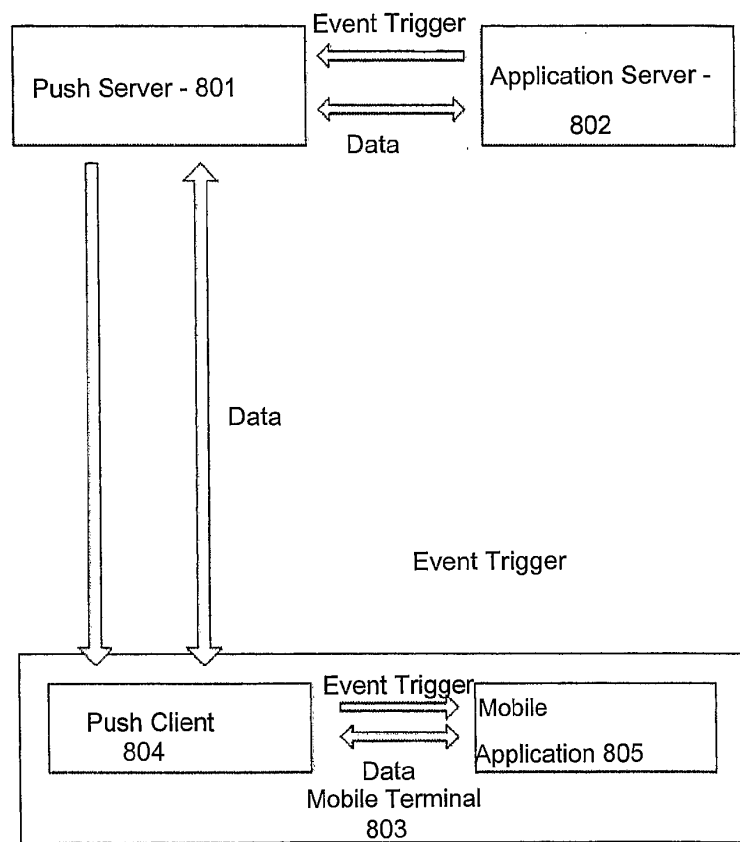
10/15

Figure 7



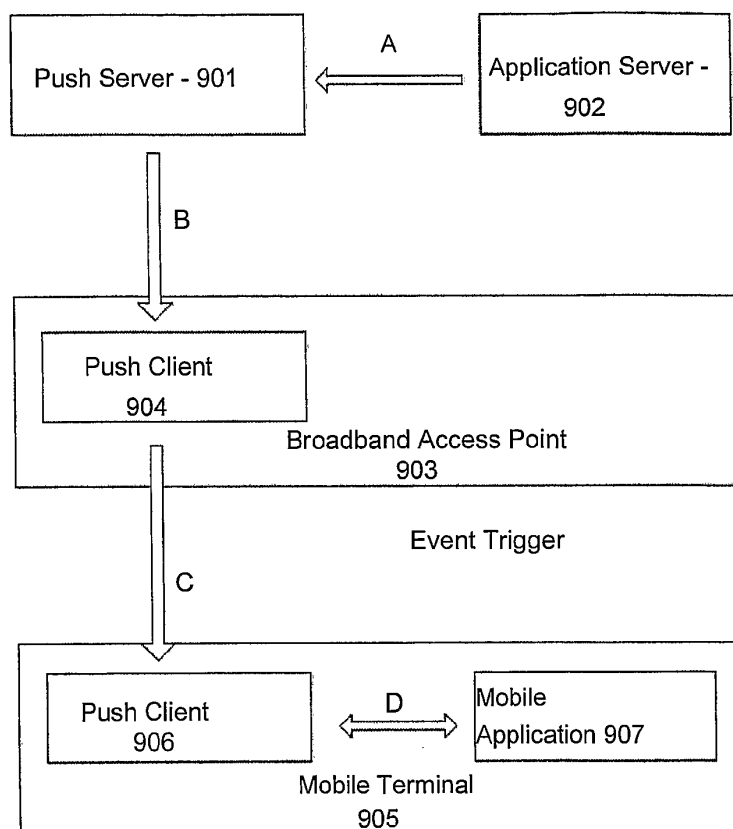
11/15

Figure 8



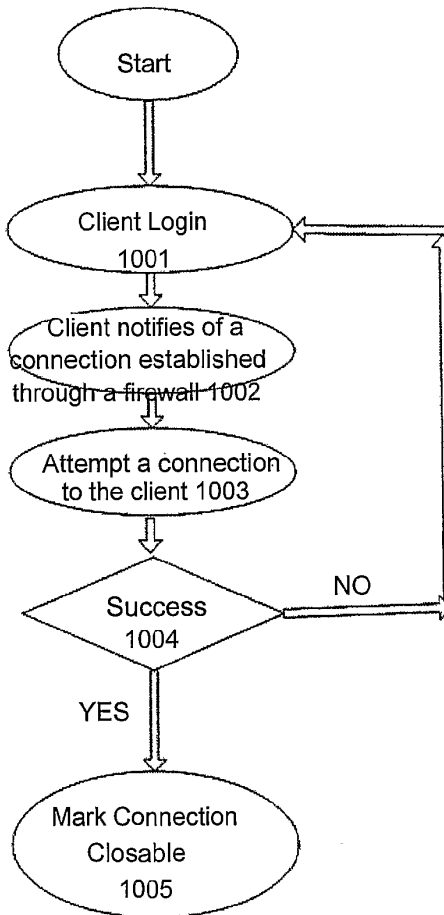
12/15

Figure 9



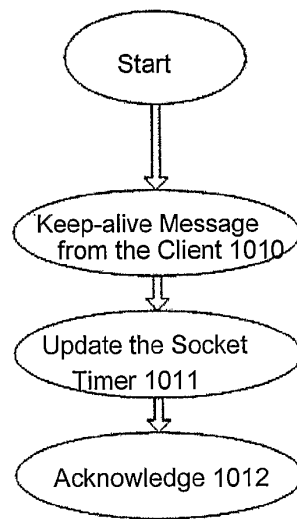
13/15

Figure 10A



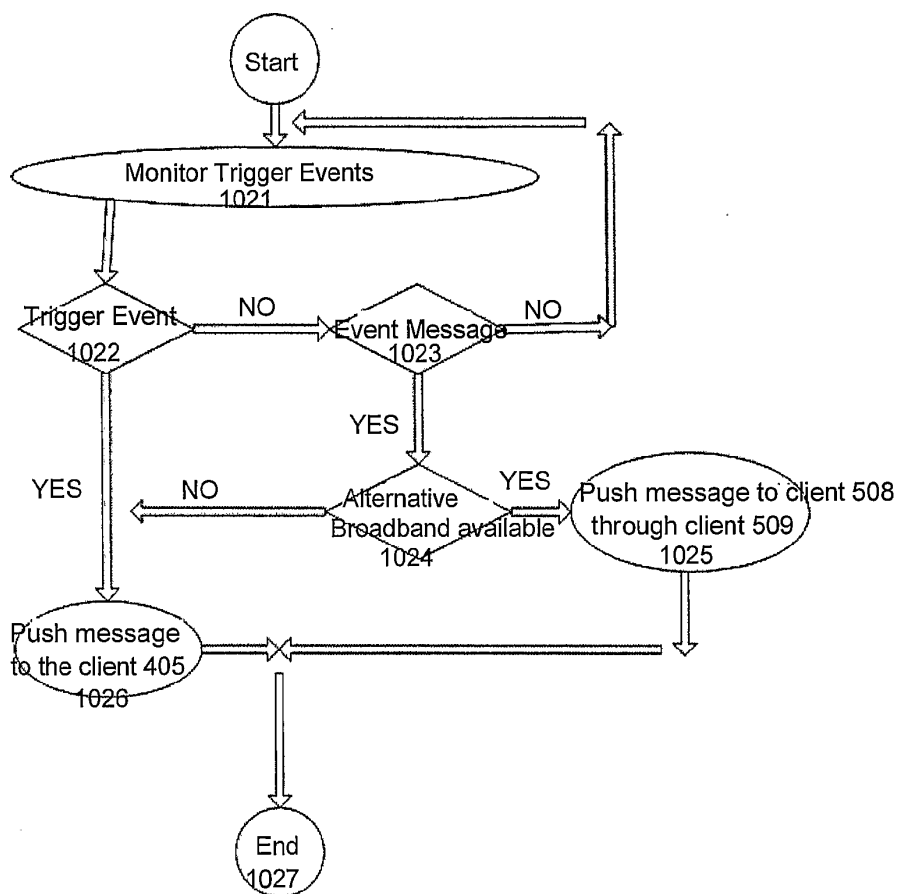
14/15

Figure 10B



15/15

Figure 10C



SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2006/050032

A. CLASSIFICATION OF SUBJECT MATTER

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC8: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI, PAJ, INSPEC, IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2001/0005864 A1 (MOUSSEAU et al.) 28 June 2001 (28.06.2001), Abstract, paragraphs [0003], [0013], [0018], [0071], [0073], [0075]-[0082], fig. 6-9	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
Y	US 2003/0009561 A1 (SOLLEE) 09 January 2003 (09.01.2003), paragraphs [0007], [0027], [0076]	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
Y	WO 02067538 A2 (CELLTICK TECHNOLOGIES LTD et al.) 29 August 2002 (29.08.2002), Abstract, claim 6	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
A	JP 2003134566 A (AICON KK et al.) 09 May 2003 (09.05.2003), Abstract	1-37
A, P	US 2006/0009198 A1 (KASAI et al.) 12 January 2006 (12.01.2006), whole document	1-37

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

28 March 2006 (28.03.2006)

Date of mailing of the international search report

10 April 2006 (10.04.2006)

Name and mailing address of the ISA/FI
National Board of Patents and Registration of Finland
P.O. Box 1160, FI-00101 HELSINKI, Finland

Authorized officer

Seppo Ojala

Facsimile No. +358 9 6939 5222

Telephone No. +358 9 6939 5000

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050032

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2001/0005864 A1	28/06/2001	US 2005148356 A1	07/07/2005
		JP 2005100427 A	14/04/2005
		JP 2005100426 A	14/04/2005
		JP 2005056437 A	03/03/2005
		US 2004252727 A1	16/12/2004
		JP 2004220622 A	05/08/2004
		US 2004073619 A1	15/04/2004
		US 2004024824 A1	05/02/2004
		US 2003187938 A1	02/10/2003
		US 2003050987 A1	13/03/2003
		US 2003005066 A1	02/01/2003
		US 2003018816 A1	23/01/2003
		US 2002194285 A1	19/12/2002
		US 2002049818 A1	25/04/2002
		US 2002029258 A1	07/03/2002
		EP 1282957 A2	12/02/2003
		EP 1273136 A2	08/01/2003
		EP 1273135 A2	08/01/2003
		CN 1436413 A	13/08/2003
		WO 0178342 A2	18/10/2001
		WO 0178341 A2	18/10/2001
		WO 0178319 A2	18/10/2001
		CA 2343932 A1	10/10/2001
		CA 2343905 A1	10/10/2001
		CA 2343648 A1	10/10/2001
		AU 5206001 A	23/10/2001
		AU 5020401 A	23/10/2001
		AU 5020101 A	23/10/2001
		US 2001054115 A1	20/12/2001
		US 2002120696 A1	29/08/2002
		US 2001005857 A1	28/06/2001
		US 2001005861 A1	28/06/2001
		US 2001004744 A1	21/06/2001
		US 2001005860 A1	28/06/2001
		US 2001013071 A1	09/08/2001
		US 2001009015 A1	19/07/2001
		MX PA00011592 A	17/10/2002
		NO 20005917 A	26/01/2001
		US 6463463 B1	08/10/2002
		US 6779019 B1	17/08/2004
		US 6463464 B1	08/10/2002
		US 6701378 B1	02/03/2004
		NZ 528050 A	28/01/2005
		NZ 508305 A	30/04/2004
		JP 2002517947T T	18/06/2002
		EP 1082839 A2	14/03/2001
		EP 1320221 A2	18/06/2003
		EP 1315336 A1	28/05/2003

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050032

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
		EP 1206073 A2	15/05/2002
		EP 1126662 A2	22/08/2001
		EP 1124352 A2	16/08/2001
		EP 1098481 A2	09/05/2001
		EP 1096727 A2	02/05/2001
		EP 1096726 A2	02/05/2001
		EP 1096725 A2	02/05/2001
		CN 1304608 A	18/07/2001
		WO 9963709 A2	09/12/1999
		CA 2333881 A1	09/12/1999
		AU 3924499 A	20/12/1999
		AU 758302B B2	20/03/2003
		CA 2511594 A1	29/11/1999
		CA 2367135 A1	29/11/1999
		CA 2356324 A1	29/11/1999
		CA 2356073 A1	29/11/1999
		CA 2356046 A1	29/11/1999
		CA 2356038 A1	29/11/1999
		CA 2356004 A1	29/11/1999
		CA 2245157 A1	29/11/1999
		US 6219694 B1	17/04/2001
<hr/>			
US 2003/0009561 A1	09/01/2003	WO 02103981 A2	27/12/2002
		EP 1446929 A2	18/08/2004
<hr/>			
WO 02067538 A2	29/08/2002	RU 2004116910 A	10/10/2005
		US 2004078427 A1	22/04/2004
		EP 1362491 A2	19/11/2003
		CN 1493165 A	28/04/2004
<hr/>			
JP 2003134566 A	09/05/2003	None	
<hr/>			
US 2006/0009198 A1	12/01/2006	JP 2005108012 A	21/04/2005
<hr/>			

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2006/050032

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.
H04L 12/56 (2006.01)
H04L 29/08 (2006.01)
H04Q 7/22 (2006.01)



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	12/31/2024	12184700	RALEP007C11C3C2C3C2C1C1C1	5850

106963 7590 12/11/2024
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at <https://patentcenter.uspto.gov/>. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at <https://certifiedcopycenter.uspto.gov/index.html>. The Certified Copy Center may be reached at (800)972-6382.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment is 302 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Center (<https://patentcenter.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PATENT CENTER site <https://patentcenter.uspto.gov> for additional inventors):

Gregory G. Raleigh, Incline Village, NV;

APPLICANT(s) (Please see PATENT CENTER site <https://patentcenter.uspto.gov> for additional applicants):

Headwater Research LLC, Tyler, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	42	7082422	B1	2006-07-25	Zirngibl et al.	
	43	7084775	B1	2006-08-01	Smith, Michael R.	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7095754	B2	2006-08-22	Benveniste, Mathilde	
	46	7102620	B2	2006-09-05	Harries, Andrew Stanely Guy et al.	
	47	7110753	B2	2006-09-19	Campen, Kenneth Brian	
	48	7113780	B2	2006-09-26	Mckenna Daniel et al.	
Change(s) applied to document /J.E./ 9/3/2024	49	7113997		2012-08-26 09/2006	Jayapalan, Jay et al.	
	50	7120133	B1	2006-10-10	Joo et al.	
	51	7133386	B2	2006-11-07	Holur et al.	
	52	7133695	B2	2006-11-07	Beyda, William J.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit			
	Examiner Name			
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C		

/	9	9032192	B2	2015-05-12	Frank	
	10	8620988		2013-12-31	Sohm	
	11	5581704		1996-12-03	Barbara	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S. PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/	1	20030096625	A1	2003-05-22	Lee et al.	
Changes(s) applied to document, /J.E./ 9/3/2024	2	20050207379	B2	2011-04-12 09/2005	Shen et al.	
	3	20090037270	A1	2009-02-05	Patro	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/	1	1909463	EP	B1	2016-09-21	Hwang et al.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		3687	
	Examiner Name		Unknown	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	3	20090282256		2009-11-12	Rakic	
	4	20040122907		2004-06-24	Chou	
	5	20040105431		2004-06-03	Monjas-Llorente	
	6	20070214245		2007-09-13	Hämäläinen	
	7	20050207379		2005-09-22	Shen	
	8	20060190720		2006-08-24	Ozaki	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
Change(s) applied to document, /J.E./ 9/3/2024	1	2006077283	WO		07/2006	Houghton		☐
	2	2008048075	WO		04/2008	Lee		☐
	3	1853044	EP		11/2007	Shenfield		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	11/13/2024 03:08:47 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	67951242	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C 1C1C1_Issue_Fee_Nov_13_ 24.pdf	5	-	337 KB
RALEP007C11C3C2C3C2 C1C1C1_Issue_Fee_Nov_ 13_24-TRAN.LET.pdf	(1-1) 1	Transmittal Letter	33 KB
RALEP007C11C3C2C3C2 C1C1C1_Issue_Fee_Nov_ 13_24-IFEE.pdf	(2-5) 4	Issue Fee Payment (PTO-85B)	311 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
----------	-------------------------

RALEP007C11C3C2C3C2C1C 1C1_Issue_Fee_Nov_13_24.pdf	1E43FD4613DCDEAC4E0E46E74FB0FAD05F719BCA9388FDA 9B8E84C582405A5C1FF233D11ACB27E725E4611239598218E A899AE8DF1228478EA8A29B4F6852224
RALEP007C11C3C2C3C2C1C 1C1_Issue_Fee_Nov_13_24- TRAN.LET.pdf	8A42C7BB3004C490545D5026AF54136673EF5CD40BC1F3A28 8A4B2C98F5C2878040A34F52E25EE1A05BA2CBD153C090E8 DB817AD4268F29FCA1CBA9DA62FD211
RALEP007C11C3C2C3C2C1C 1C1_Issue_Fee_Nov_13_24- IFEE.pdf	23D631362D9B1F458D0813AC2195E61A0C93E334C71E2AA1D 5EC39C117A05579FB021BA15607E2D1402726D1794C4C36B5 29512198D119279588EEED2CE7DA30

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: November 13, 2024

To: United States Patent and Trademark Office
Examiner: Murillo Garcia, Fabricio R.; Art Unit: 2633

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 5

Message:

Enclosed, please find the Issue Fee.

Credit Card payment in the amount of **\$480.00** as the required Issue fee is hereby included with this filing.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account No. **50-0731**.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): **Raleigh**

Application Serial No.: **17/577,237**

Filed: **1/17/2022**

Title: **Automated Device Provisioning and
Activation**

Group Art Unit: 2633

Examiner: Murillo Garcia, Fabricio R.

Notice of Allowance: November 13, 2024

ISSUE FEE

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

Enclosed, please find the completed "Issue Fee Transmittal" form and a "**Payment by Credit Card**" in the amount of **\$480.00** to cover the issue fee. The drawings filed in the present application have been accepted as formal drawings by the Examiner.

COMMENTS ON STATEMENTS OF REASONS FOR ALLOWANCE

The Applicant recognizes that in accordance with M.P.E.P. § 1302.14, the reasons for allowance provided by the Examiner do not necessarily include all of the reasons why the claims are allowed. The Applicant does not concede that the stated reasons for allowance are the only grounds for patentability of the allowed claims or that any element excluded from the Examiner's Reasons for Allowance is taught or suggested by the art of record.

Further, the Applicant does not concede that all of the elements identified by the Examiner are required to distinguish the prior art of record or to satisfy the requirements of 35 U.S.C. § 112. In addition, the Examiner does not assert, and the Applicant would not agree, that the stated reasons for allowance have any bearing on the patentability of claims in any other applications.

Each dependent claim stands on its own and is allowable based on its own elements or in combination with one or more elements recited in its base claim(s). The combination of elements need not include all of the elements identified in the stated reasons for allowance.

The Commissioner is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number **50-0731**.

An early issuance of the present application is respectfully requested.

Respectfully submitted,
Farjami & Farjami LLP

By: /Farshad Farjami/
Farshad Farjami, Esq.
Reg. No. 41,014

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Ste. 360
Mission Viejo, CA 92691
Tel: (949) 282-1000
Fax: (949) 282-1002

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

November 13, 2024
Date

Evan C. Gunderman
Name

/evan c. gunderman/
Signature

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 11/08/2024
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

Evan C. Gunderman	(Typed or printed name)
/Evan C. Gunderman/	(Signature)
November 13, 2024	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

17/577,237

01/17/2022

Gregory G. Raleigh

RALEP007C11C3C2C3C2C1C1C1

5850

TITLE OF INVENTION: Automated Device Provisioning and Activation

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	02/10/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
MURILLO GARCIA, FABRICIO R	2633	455-406000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Farjami & Farjami LLP

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

Headwater Research LLC

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

Tyler, TX

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☒ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. **50-0731**

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Farshad Farjami/

Date November 13, 2024

Typed or printed name Farshad Farjami

Registration No. 41014



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	11/13/2024 03:08:47 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	67951242	AUTHORIZED BY	Michael Farjami
CUSTOMER #	106963	FILING DATE	01/17/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Gregory G. Raleigh

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 5006	E2024ACF10427604	Evan Gunderman

PRE-AUTHORIZED ACCOUNT	PRE-AUTHORIZED CATEGORY
500731	37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees); 37 CFR 1.21 (Miscellaneous fees and charges)

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2501	UTILITY ISSUE FEE	480.00	1	480.00
TOTAL AMOUNT:				\$480.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

106963 7590 11/08/2024
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

EXAMINER

MURILLO GARCIA, FABRICIO R

ART UNIT PAPER NUMBER

2633

DATE MAILED: 11/08/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007/C11C3C2C3C2C1C1C1	5850

TITLE OF INVENTION: Automated Device Provisioning and Activation

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	02/10/2025

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 11/08/2024

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

17/577,237

01/17/2022

Gregory G. Raleigh

RALEP007C11C3C2C3C2C1C1C1

5850

TITLE OF INVENTION: Automated Device Provisioning and Activation

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	02/10/2025

EXAMINER	ART UNIT	CLASS-SUBCLASS
MURILLO GARCIA, FABRICIO R	2633	455-406000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850
106963	7590	11/08/2024	EXAMINER	
Headwater Research LLC C/O Farjami & Farjami LLP 26522 La Alameda Ave., Suite 360 Mission Viejo, CA 92691			MURILLO GARCIA, FABRICIO R	
			ART UNIT	PAPER NUMBER
			2633	
DATE MAILED: 11/08/2024				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.** Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).

<https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to:

- 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
- 2) a federal, state, local, or international agency, in response to its request;
- 3) a contractor of the USPTO having need for the information in order to perform a contract;
- 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
- 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
- 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
- 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
- 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
- 9) the Office of Personnel Management (OPM) for personnel research purposes; and
- 10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 17/577,237	Applicant(s) Raleigh, Gregory G.	
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 09/13/2024.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 2-16. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some* c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)	5. ☒ Examiner's Amendment/Comment
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.	6. ☒ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____.	

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on **13 September 2024** has been entered.

Information Disclosure Statement

The IDS submitted on **05 September 2024** is in compliance and has been considered. Examiner notes that, given the quantity and length of the references, only a cursory review has been performed, based on feedback received by the Applicant via Applicant's representative, Mr. Farshad Farjani, on interview held on **03 October 2024**.

Response to Arguments

Following response to arguments is based on Applicant's arguments filed on **18 July 2024**.

Regarding Previous Claim Objections

Previous objection to claims **2, 4, 7, 9, 12, 14** has been withdrawn in view of the amendments to the objected claims.

Regarding Previous Rejection Under 35 USC § 112

Previous rejection of claims **2-16** has been withdrawn in view of the amendment to the rejected claims.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for the following examiner's amendment was given in a telephone interview with **Farshad Farjami (Reg. No. 41,014) on 07 August 2024.**

In the claims, the Examiner's Amendment is as follows:

Claims **2, 7, 12** have been amended as follows:

Claim 2 (Currently Amended): A network message server adapted to communicate with a mobile end-user device having a plurality of applications, the

network message server comprising:

one or more processors configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the received request corresponding to a first application of the plurality of **applications**;

generate an Internet data message based on the received request, the **generated** Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and **for** forwarding the application data in the transmitted Internet data message to the first application mapped by the mobile end-user device to the first application identifier.

Claim 7 (Currently Amended): A method for use by a network message server adapted to communicate with a mobile end-user device having a plurality of applications, the method comprising:

providing a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receiving a request to transmit application data, the received request corresponding to a first application of the plurality of **applications**;

generating an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and

transmitting, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and **for** forwarding the application data in the transmitted Internet data message to the first application mapped by the mobile end-user device to the first application identifier.

Claim 12 (Currently Amended): A network system comprising:

a mobile end-user device having a plurality of applications;

a network message server adapted to communicate with the mobile end-user device, the network message server configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the received request corresponding to a first application of the plurality of **applications**;

generate an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device;

the mobile end-user device configured to:

receive the transmitted Internet data message from the network message server;

map the first application identifier included in the received Internet data message to the first application corresponding to the first application identifier; and

forward the application data in the received Internet data message to the first application mapped by the mobile end-user device to the first application identifier.

Allowable Subject Matter

Claims **2-16** are allowed.

The following is an examiner's statement of reasons for allowance:

Regarding claim 2, the prior art of record does not show or suggest the combination of the following limitations: *"transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and forward the application data in the transmitted Internet data message to the first application mapped by the mobile end-user device to the first application identifier"*.

Regarding claims 7 and 12, these claims are also allowed as they incorporate limitations similar to those set forth in independent claim 2.

It is the claim, taken as a whole, including the interrelationships and interconnections between the various claimed elements, that which make it allowable

over the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Alharayeri US Patent Application Publication No. 2016/0135014 teaches location-based discovery of network members by personal attributes using dynamic and static location data.
2. Newell US Patent Application Publication No. 2009/0328197 teaches user validation using images.
3. Shima et al. US Patent Application Publication No. 2016/0105438 teaches system, method, and apparatus for authentication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FABRICIO R MURILLO GARCIA whose telephone number is (571)270-5708. The examiner can normally be reached 9-5pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sam K Ahn can be reached on 5712723044. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

November 2, 2024

/FABRICIO R MURILLO GARCIA/
Primary Examiner, Art Unit 2633

<i>Examiner-Initiated Interview Summary</i>	Application No. 17/577,237	Applicant(s) Raleigh, Gregory G.		
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633	AIA (First Inventor to File) Status No	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
FABRICIO R MURILLO GARCIA	Primary Examiner	Telephonic
Farshad Farjami (Reg. No. 41,014)	Attorney of Record	

Date of Interview: 03 October 2024

Issues Discussed:

Other

Discussed about the relevance of the filed IDS given the quantity and length of the references. The Examiner thanks Applicant's representative, Mr. Farjami, for his professionalism.

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
<p>Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04</p> <p>Please further see: MPEP 713.04 Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b) 37 CFR § 1.2 Business to be transacted in writing</p>	

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

<i>Notice of References Cited</i>	Application/Control No. 17/577,237		Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.	
	Examiner FABRICIO R MURILLO GARCIA		Art Unit 2633	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20160135014-A1	2016-05-12	Alharayeri; Ramzi	H04L67/306	455/456.3
*	B	US-20090328197-A1	2009-12-31	Newell; Mark Dwight	G06F21/36	345/168
*	C	US-20160105438-A1	2016-04-14	SHIMA; Taira	H04L63/0884	726/4
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC						
Symbol					Type	Version
H04L	/	63	/	20	F	2013-01-01
G06Q	/	10	/	06375	I	2013-01-01
G06Q	/	20	/	102	I	2013-01-01
G06Q	/	20	/	20	I	2013-01-01
G06Q	/	20	/	40	I	2013-01-01
G06Q	/	30	/	0207	I	2013-01-01
G06Q	/	30	/	0283	I	2013-01-01
G06Q	/	30	/	0284	I	2013-01-01
G06Q	/	30	/	04	I	2013-01-01
G06Q	/	30	/	0601	I	2013-01-01
G06Q	/	40	/	00	I	2013-01-01
H04L	/	12	/	14	I	2013-01-01
H04L	/	41	/	0893	I	2013-01-01
H04M	/	15	/	00	I	2013-01-01
H04M	/	15	/	58	I	2013-01-01
H04W	/	88	/	08	I	2013-01-01
H04L	/	63	/	0236	I	2013-01-01
H04L	/	67	/	306	I	2013-01-01
G06Q	/	40	/	12	I	2013-01-01
H04W	/	4	/	50	I	2018-02-01
H04W	/	12	/	037	I	2021-01-01
H04L	/	67	/	55	I	2022-05-01
H04L	/	67	/	63	I	2022-05-01
H04L	/	41	/	5003	I	2013-01-01
H04W	/	4	/	24	I	2013-01-01
G06F	/	15	/	177	I	2013-01-01
G06Q	/	30	/	0241	I	2013-01-01
H04L	/	9	/	32	I	2013-01-01
H04L	/	63	/	10	I	2013-01-01
H04W	/	28	/	02	I	2013-01-01
H04W	/	12	/	08	I	2013-01-01

Use images from artifact folder? ☒ Yes ☐ No			
NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner) _____ (Date) _____		02 October 2024 O.G. Print Claim(s) 2	O.G. Print Figure 3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC						
Symbol				Type	Version	
H04L	/	47	/	2408	I	2013-01-01
H04L	/	63	/	08	I	2013-01-01
H04W	/	8	/	20	I	2013-01-01
H04W	/	28	/	12	I	2013-01-01
H04W	/	48	/	14	I	2013-01-01
H04W	/	4	/	20	I	2013-01-01
H04W	/	12	/	00	I	2013-01-01
H04M	/	15	/	88	I	2013-01-01
H04W	/	28	/	0268	I	2013-01-01
H04M	/	15	/	61	I	2013-01-01
H04W	/	24	/	08	I	2013-01-01
H04W	/	12	/	02	I	2013-01-01
H04L	/	51	/	046	I	2013-01-01
H04L	/	63	/	0428	I	2013-01-01
H04W	/	4	/	12	I	2013-01-01
H04W	/	4	/	18	I	2013-01-01
H04W	/	8	/	18	I	2013-01-01
H04W	/	72	/	0453	I	2013-01-01
H04L	/	47	/	20	I	2013-01-01
H04W	/	28	/	0215	I	2013-01-01
H04W	/	4	/	02	I	2013-01-01
G06Q	/	10	/	06315	I	2013-01-01
H04L	/	41	/	0806	I	2013-01-01
H04L	/	41	/	5054	I	2013-01-01
H04M	/	15	/	80	I	2013-01-01
H04L	/	63	/	04	I	2013-01-01
H04L	/	9	/	3247	I	2013-01-01
H04L	/	63	/	0892	I	2013-01-01
H04L	/	67	/	145	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
H04L	/	63	/	0853	I	2013-01-01

Use images from artifact folder? ☒ Yes ☐ No			
NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 2	O.G. Print Figure 3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC						
Symbol					Type	Version
H04W	/	48	/	16	I	2013-01-01
H04L	/	41	/	5025	A	2013-01-01
H04M	/	2215	/	0188	A	2013-01-01
H04L	/	67	/	34	A	2013-01-01
H04W	/	8	/	02	A	2013-01-01
Y02P	/	90	/	80	A	2015-11-01
H04L	/	67	/	564	A	2022-05-01
H04W	/	84	/	04	A	2013-01-01
H04W	/	84	/	12	A	2013-01-01
H04W	/	88	/	06	A	2013-01-01
H04W	/	84	/	042	A	2013-01-01
H04L	/	41	/	0876	A	2013-01-01

CPC Combination Sets						
Symbol				Type	Set	Ranking
	/		/			

Use images from artifact folder? ☒ Yes ☐ No			
NONE (Assistant Examiner)		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner)		02 October 2024 (Date)	O.G. Print Claim(s) 2
			O.G. Print Figure 3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

INTERNATIONAL CLASSIFICATION				
CLAIMED				
H04L9/40	/	9	/	40
G06Q10/0637	/	10	/	0637
G06Q20/10	/	20	/	10
G06Q20/20	/	20	/	20
G06Q20/40	/	20	/	40
G06Q30/0207	/	30	/	0207
G06Q30/0283	/	30	/	0283
G06Q30/04	/	30	/	04
G06Q30/0601	/	30	/	0601
G06Q40/00	/	40	/	00
H04L12/14	/	12	/	14
H04L41/0893	/	41	/	0893
H04M15/00	/	15	/	00
H04W88/08	/	88	/	08
H04L67/306	/	67	/	306
G06Q40/12	/	40	/	12
H04W4/50	/	4	/	50
H04W12/037	/	12	/	037
H04L67/55	/	67	/	55
H04L67/63	/	67	/	63
H04L41/5003	/	41	/	5003
H04W4/24	/	4	/	24
G06F15/177	/	15	/	177
G06Q30/0241	/	30	/	0241
H04L9/32	/	9	/	32
H04W28/02	/	28	/	02
H04W12/08	/	12	/	08
H04L47/2408	/	47	/	2408
H04W8/20	/	8	/	20
H04W28/12	/	28	/	12
H04W48/14	/	48	/	14

Use images from artifact folder? ☒ Yes ☐ No			
NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	02 October 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	2	3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04W4/20	/	4	/ 20
H04W12/00	/	12	/ 00
H04W24/08	/	24	/ 08
H04W12/02	/	12	/ 02
H04L51/046	/	51	/ 046
H04W4/12	/	4	/ 12
H04W4/18	/	4	/ 18
H04W8/18	/	8	/ 18
H04W72/0453	/	72	/ 0453
NON-CLAIMED			
	/		/

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
455	406

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

Use images from artifact folder? ☒ Yes ☐ No			
NONE (Assistant Examiner)		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner)		02 October 2024 (Date)	O.G. Print Claim(s) 2
			O.G. Print Figure 3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
-	1		10												
	2		11												
	3		12												
	4		13												
	5		14												
	6		15												
	7		16												
	8														
	9														

Use images from artifact folder? ☒ Yes ☐ No			
NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	15	
/FABRICIO R MURILLO GARCIA/	02 October 2024	O.G. Print Claim(s)	O.G. Print Figure
Primary Examiner, Art Unit 2633		2	3
(Primary Examiner)	(Date)		

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC - Searched*		
Symbol	Date	Examiner
G06F15/177	03/09/2024	FM
H04W28/0215	03/09/2024	FM

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
455/406		03/09/2024	FM

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

Search Notes		
Search Notes	Date	Examiner
East (See Attachment)	03/09/2024	FM
Inventor Search (search for double patenting)	03/09/2024	FM
Non Patentable Literature	03/09/2024	FM
455/406 - See Attached East Search	03/09/2024	FM
G06F15/177 - See Attached East Search	03/09/2024	FM
H04W28/0215 - See Attached East Search	03/09/2024	FM
Updated	06/25/2024	FM
Updated	08/06/2024	FM
455/406 Interference Search - See Attached East Search	08/06/2024	FM
G06F15/177 Interference Search - See Attached East Search	08/06/2024	FM
H04W28/0215 Interference Search - See Attached East Search	08/06/2024	FM
Updated	10/02/2024	FM

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
455/406		08/06/2024	FM
G06F15/177		08/06/2024	FM
H04W28/0215		08/06/2024	FM

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	1	"17577237"	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:06 AM
L2	633	((("RALEIGH") near3 ("Gregory"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/03/09 06:10 AM
L3	1	((US-20220279021-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:19 PM
L4	3098	(store) WITH ((device) near2 (credential))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:36 PM
L5	2	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L6	0	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal) WITH (activate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L7	30	("6178511" "6243816" "7249182" "7296036" "7310515" "7346855" "7353462" "8472874" "8606854" "20040009750" "20040113807" "20050026594" "20050076124" "20050193093" "20050281237" "20060063548" "20060234631" "20070021111" "20070167136" "20070168425" "20070242814" "20070260751" "20080051033" "20080108308" "20090209202").pn. OR ("9357352").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:38 PM
L8	4	((US-11304026-B2 OR US-10963844-B2 OR US-10250549-B2 OR US-9609673-B2).did. AND USPT.dbnm.)	(USPAT)	OR	ON	ON	2024/03/09 06:38 PM
L9	4	((US-8606854-B2 OR US-8472874-B2).did.	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM

L10	4	AND USPT.dbnm.) OR ((US-20090209202-A1 OR US-20080108308- A1).did. AND PGPB.dbnm.) ((US-7353462-B2 OR US-7346855-B2 OR US-7296036-B2).did. AND USPT.dbnm.) OR ((US-20080051033- A1).did. AND PGPB.dbnm.)	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L11	4	((US-20070260751-A1 OR US-20070242814- A1 OR US- 20070167136-A1 OR US-20070168425- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L12	4	((US-20070021111-A1 OR US-20060234631- A1 OR US- 20060063548-A1 OR US-20050281237- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L13	41	("6867733" "7418268" "7686217" "7847684" "8010131" "8108414" "8655385" "8688143" "8892130" "9173245" "9203857" "9226105" "9268920" "9357352" "9485211" "9830562" "9940402" "10013489" "10049400" "10075822" "10078696" "10264609" "10575138" "10599390" "20040116106" "20100313142" "20130316735" "20130331087" "20140162698" "20150058427" "20150080027" "20150088672" "20150365787" "20150378587" "20160261985" "20160334545" "20160364811" "20180176166"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:39 PM

L14	2	"20190014220" "20190215660" "20210173880").pn. OR ("11304026").urpn. AND (PGPB USPT USOC).dbnm. (storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L15	5	(stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L16	5	(save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L17	5	(saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L18	5	(saved saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L19	6	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L20	30	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L21	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L22	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM

L23	72	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L24	75	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L25	759	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L26	762	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L27	128	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L28	88	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L29	78	(user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L30	66	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L31	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L32	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activae)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L33	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L34	1	(user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L35	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L36	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start begin)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:44 PM
L37	1	("2022/0124167").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:45 PM
L38	2	((US-20220279021-A1 OR US-20160135014- A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/03/09 06:45 PM
L39	1	(saved saving save stored storing store) near10 ((device sensor)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L40	1	near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start begin beginning)) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began begin beginning))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L41	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began begin beginning))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L42	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began began begin beginning))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L43	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start started began begun begin beginning))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L44	1	near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L45	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L46	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L47	4	starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) WITH ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L48	3	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L49	4	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L50	15	(saved saving save	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09

		stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) WITH (initiated initiating running starting run activate initiate start started began begun begin beginning)					06:56 PM
L51	4	((US-20220124167-A1 OR US-20200275225- A1 OR US- 20170006034-A1).did. AND PGPB.dbnm.) OR ((US-9554061-B1).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:59 PM
L52	3	((US-20140373012-A1 OR US-20140337940- A1 OR US- 20130191885-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:59 PM
L53	24	("6757837" "6882712" "6889510" "7355730" "20020082924" "20060236325" "20070225828" "20080167127" "20080167128" "20080167133" "20090078760" "20100112997" "20100268401" "20110113087" "20110202798" "20110294466" "20120129492" "20120221893" "20120226619" "20120324067" "20140028449" "20140173059").pn. OR ("9129127").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM
L54	88	("6564056" "7664707" "7908401" "8311513" "8447696" "8974544" "9129127" "9141150" "9183380" "9204298" "9246921" "9489250"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM

		"9507950" "9524174" "9531559" "9575477" "20040125782" "20050246243" "20080062258" "20080204199" "20090023395" "20100031371" "20100094981" "20110145927" "20130067551" "20130171981" "20130191885" "20130254437" "20130304795" "20130311684" "20140040989" "20140098247" "20140245765" "20140263612" "20140266669" "20140266679" "20140277597" "20140279109" "20140282486" "20140304632" "20140313048" "20140344454" "20140359042" "20140376528" "20150006686" "20150033305" "20150038129" "20150040246" "20150052578" "20150061859" "20150081928" "20150097689" "20150100618" "20150109104" "20150160935" "20150163412" "20150177705" "20150198938" "20150215337" "20150222578" "20150261954" "20150279134" "20150304171" "20150309548" "20150324179" "20150364028" "20160014108" "20160063854" "20160098362" "20160099972" "20160103494" "20160109864"				
--	--	--	--	--	--	--

		"20160119742" "20160142258" "20160142532" "20160294602" "20160337945" "20160351036" "20160380987" "20170019264" "20170034156" "20170034158" "20170046173" "20170048712" "20170078298" "20170093860" "20170099560" "20170109998").pn. OR ("10157271").urpn. AND (PGPB USPT USOC).dbnm.					
L55	4	((US-20170109998-A1 OR US-20170099560- A1 OR US- 20170093860-A1).did. AND PGPB.dbnm.) OR ((US-9575477-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:00 PM
L56	1	((US-20160135014- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 07:37 PM
L57	1	"8839388".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:49 PM
L58	1	"9037127".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:54 PM
L59	1	"9232403".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:56 PM
L60	1	"9532161".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:57 PM
L61	1	"9641957".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:58 PM
L62	1	"10321320".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:59 PM
L63	1	"11228617".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 08:00 PM
L64	8	"20090292815"	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 08:06 PM
L65	1	((US-20090292815- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 09:27 PM
L66	806072	(memory WITH instructions) AND ;65	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 09:27 PM
L67	0	(memory WITH instructions) AND L65	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 09:27 PM
L68	1	(memory SAME	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09

L69	2126	instructions) AND L65 ((secure) near2(internet)) WITH (application)	(US-PGPUB; USPAT)	OR	ON	ON	09:28 PM 2024/06/25 03:05 AM
L70	7	((secure) near2(internet)) WITH (application) WITH (communication ADJ device)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L71	8	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L72	14	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L73	56	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:08 AM
L74	78	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L75	90	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L76	90	((secure) near2(internet)) WITH (application) WITH	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM

L77	103	((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld cellphone))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L78	103	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld cellphone smartphone))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L79	103	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L80	144	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM

L81	3	terminal) (mobile ADJ device)) ((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L82	12	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L83	16	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L84	16	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM

L85	16	cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying) ((secure) near2(internet)) WITH (app application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L86	24	((secure) near2(internet)) SAME (app application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L87	64	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L88	110	((secure) near2(internet)) SAME	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM

L89	20	(app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) ((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:13 AM
L90	20	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:13 AM
L91	19	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:14 AM

L92	22966	ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data) (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/06 02:35 AM
L93	5	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)) AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:35 AM
L94	5	((US-20220279021-A1 OR US-20160135014- A1 OR US- 20090292815-A1 OR US-20090328197- A1).did. AND PGPB.dbnm.) OR ((US- 8839388-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/06 04:31 AM
L95	1	"20220279021"	(US-PGPUB)	OR	ON	ON	2024/08/06 04:35 AM
L96	247	"8,285,850" "5,987,611" "6,947,723" "7,454,446" "8,799,242" "7,860,964" "5,481,735" "5,764,693"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/02 03:36 AM
L97	268	"20070149252" "20060039354" "20060075090" "20060019632" "20060203739" "20080026787"	(US-PGPUB; USPAT)	OR	ON	ON	2024/10/02 03:37 AM

L98	115	"20080122796" "20090217065" "20080002652"	(USPAT)	OR	ON	ON	2024/10/02 03:37 AM
L99	34	"8,285,850" "5,987,611" "6,947,723" "7,454,446" "8,799,242" "7,860,964" "5,481,735" "5,764,693"	(US-PGPUB)	OR	ON	ON	2024/10/02 03:37 AM
L100	1	"20070149252" "20060039354" "20060075090" "20060019632" "20060203739" "20080026787" "20080122796" "20090217065" "20080002652" "20070117550"	(US-PGPUB)	OR	ON	ON	2024/10/02 03:38 AM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N2	1	((secure) near2(internet)) NEAR10 (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:36 AM
N3	0	((secure) near2(internet)) NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:36 AM

N4	0	cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.) (((secure) near2(internet)) NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) NEAR10 (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:36 AM
N5	0	(((secure) near2(internet)) NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) NEAR10 (id identifier identification identifying) NEAR10 (wireless wirelessly) SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:37 AM
N6	0	(((secure) near2(internet))	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:37 AM

N7	0	NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) NEAR10 (id identifier identification identifying) NEAR10 (wireless wirelessly) NEAR10 (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.) ((saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)) AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:40 AM
N8	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:42 AM
N9	0	((saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:42 AM

N10	0	(mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate)) AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.) ((saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:42 AM
-----	---	---	-------------------	----	----	----	------------------------

Doc code: IDS

PTO/SB/08a (01-22)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	8,285,850		2012-10-09	Jones; Nathan et al.	
	2	5,987,611		1999-11-16	Freund; Gregor	
	3	6,947,723		2005-09-20	Gumani; Roger et al.	
	4	7,454,446		2008-11-18	Leung; Albert et al.	
	5	8,799,242		2014-08-05	Leonard; Glenda Ann et al.	
	6	7,860,964		2010-12-28	Brady; Mark et al.	
	7	5,481,735		1996-01-02	Mortensen; Craig et al.	
	8	5,764,693		1998-06-09	Taylor; Bryan et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070149252		2007-06-28	Jobs; Steven P. et al.	
	2	20060039354		2006-02-23	Rao; Goutham P. et al.	
	3	20060075090		2006-04-06	Bocking; Andrew D. et al.	
	4	20060019632		2006-01-26	Cunningham; Ivy et al.	
	5	20060203739		2006-09-14	Padmanabhan; Venkata N. et al.	
	6	20080026787		2008-01-31	Ibrahim; Brima et al.	
	7	20080122796		2008-05-29	Jobs; Steven P. et al.	
	8	20090217065		2009-08-27	Araujo, JR.; Nelson S.	
	9	20080002652		2008-01-03	Gupta; Dev V. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2633		
	Examiner Name	Murillo Garcia, Fabricio R.		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	10	20070117550		2007-05-24	Boris; Adam et al.	
--	----	-------------	--	------------	--------------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Complaint for Patent Infringement in Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2-23-cv-00641 (EDTX), Dec. 29, 2023	☐
	2	Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298	☐
	3	Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39	☐
	4	Agrawal, et. al., 2005. Policy-based management of networked computing systems. IEEE Communications Magazine, 43(10), pp. 69-75	☐
	5	Blake, et al., IETF RFC 2475, "An Architecture for Differentiated Services," December 1998, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2475 on July 29, 2023	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2633
Examiner Name	Murillo Garcia, Fabricio R.
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

6	Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024	☐
7	Damianou, et al., 2001. The ponder policy specification language. In Policies for Distributed Systems and Networks: International Workshop, POLICY 2001 Bristol, UK, January 29–31, 2001 Proceedings (pp. 18-38). Springer Berlin Heidelberg	☐
8	Stone, G.N., et al., 2001. Network policy languages: a survey and a new approach, IEEE network, 15(1), pp.10-21	☐
9	Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39), IEEE	☐
10	Simplified Policy Language (CIM-SPL). Document Number DSP0231, version, 1	☐
11	Ponnappan, et al., 2002, June. A policy based QoS management system for the IntServ/DiffServ based Internet. In Proceedings Third International Workshop on Policies for Distributed Systems and Networks (pp. 159-168), IEEE	☐
12	Gonçalves, et al., 2009, October. A graphical user interface for policy composition in CIM-SPL. In 2009 International Conference on Ultra Modern Telecommunications & Workshops (pp. 1-7), IEEE.	☐
13	Liao, S.H., 2005. Expert system methodologies and applications—a decade review from 1995 to 2004. Expert systems with applications, 28(1), pp. 93-103	☐
14	van Beek, et. al., 2004, January. Adaptive streaming of high quality video over wireless LANs. In Visual Communications and Image Processing 2004 (Vol. 5308, pp. 647-660). SPIE.	☐
15	Reeder, et al., 2007. Usability challenges in security and privacy policy-authoring interfaces. In Human-Computer Interaction— INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II 11 (pp. 141-155). Springer Berlin Heidelberg.	☐
16	Mansour, et al., 2001. Jitter control in QoS networks. IEEE/ACM Transactions On Networking, 9(4), pp.492-502.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	17	IETF RFC 793, Transmission Control Protocol, September 1981, downloaded from the Internet on August 14, 2024	☐
	18	Prasad, et. al., 1998. An overview of CDMA evolution toward wideband CDMA. IEEE communications Surveys, 1(1), pp.2-29.	☐
	19	Excerpts, Garg, "An overview of wireless systems." Wireless Communications Networking, Morgan Kaufmann, 1st edition. ISBN 123735807 (2007).	☐
	20	Li, et al., 2003, December. "Dynamic priority reallocation scheme for quality of service in IEEE 802.11e WLANs." In Multimedia Computing and Networking 2004 (Vol. 5305, pp. 83-94). SPIE	☐
	21	PETITION FOR INTER PARTES REVIEW OF UNITED STATES PATENT NO. 8,588,110, filed on August 28, 2024	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	10/02/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2633
	Examiner Name	Murillo Garcia, Fabricio R.
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-09-05
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



FARJAMI & FARJAMI LLP
An Intellectual Property Law Firm

EVAN C. GUNDERMAN
egunderman@farjami.com

October 31, 2024

Via Electronic Filing System (EFS)

Refunds Branch
Director of the United States Patent and Trademark Office
Attn: Deposit Accounts
2051 Jamieson Avenue, Suite 300
Alexandria, VA 22314

Re: Title: "Automated Device Provisioning and Activation"
Application Serial No.: 17/577,237
Amount of Charge: \$104.00; Fee Code: 2806; Date of Charge: 8/21/2024
Deposit Account No. **50-0731**
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

Dear Refunds Branch:

Please refund \$104.00 to our Deposit Account No. **50-0731**, as we believe it was charged to our deposit account in error.

One June 19, 2024 we filed an Information Disclosure Statement in the above referenced application. The Application had a Non-Final Office Action attached to it which we had not yet filed a response to, but there was no Final Office Action or Notice of Allowance issued.

However, on August 21, 2024, we were charged \$104.00 to our Deposit Account under fee code 2806 (Submission of an Information Disclosure Statement). But, because of the status of the Office Action associated with the application at the time of the IDS filing, this fee does not apply. As such, we should be refunded \$104.00 charged to our Deposit Account on August 21, 2024.

Please advise when the refund of \$104.00 will be made by way of a credit to our Deposit Account No. **50-0731**. Thank you for your assistance in this matter.

Sincerely,
FARJAMI & FARJAMI LLP

/evan c. gunderman/

Evan C. Gunderman
Paralegal

26522 La Alameda Ave., Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	10/31/2024 07:53:19 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	67804101	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1C1C Let to PTO re Refund Request for 104 Charged to DA on Aug 21 24.pdf	1	Refund Request	25 KB
RALEP007C11C3C2C3C2C1C1C1 Refund Request Form.pdf	1	Refund Request	409 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C1C Let to PTO re Refund	C3EF0570C9C2383ADE42DFD3925D12FA4F1B616075BD89B9 A693BA9F23467CFF67A4F0CFB6264833EF28E00EADEC5B0B

Request for 104 Charged to DA
on Aug 21 24.pdf

45F3D48D157FEB4962598F8555ADB342

RALEP007C11C3C2C3C2C1C
1C1 Refund Request Form.pdf

5CEF4F1769AB81C0E5F75DFC7F773C3917B95165429D3C9F2
F1D6D0BF9F3375A48BF592C911904B78F389B0E6B74A4DE17
4AEA00BBFD3609591AFA9CEEB43CD3

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

REQUEST FOR REFUND

Reference # (Patent #, Application #, Trademark Serial #, Registration #, etc.)		Title of Invention or Mark Information	
17/577,237		Automated Device Provisioning and Activation	
Attorney Docket # (if applicable)	Payment Date (mm/dd/yyyy)	Refund Request Amount	
RALEP007C11C3C2C3C2C1C1C1	08/21/2024	\$ 104.00	
Refund Option (Select one)			
☒ If approved, issue the refund to the account associated with the original payment.			
☐ If approved, and the original payment was a check, issue the refund to deposit account # _____.			
☐ If approved, and the original payment was a check, issue the refund as a U.S. Treasury check.			
Reason for Refund Request <i>Refund requests must generally be filed within 2 years of payment date (37 CFR 1.26 and 2.209)</i>			
☐ Duplicate Payment ☒ No Fee Due ☐ Office Error ☐ Other: <div></div>			
☐ Small Entity Later Established* <i>*(Must be filed within 3 months of payment date, 37 CFR 1.28. There is no refund when micro entity is later established.)</i>			
Rationale (Supporting documentation may be submitted with this form)			
One June 19, 2024 we filed an Information Disclosure Statement in the above referenced application. The Application had a Non-Final Office Action attached to it which we had not yet filed a response to, but there was no Final Office Action or Notice of Allowance issued.			
However, on August 21, 2024, we were charged \$104.00 to our Deposit Account under fee code 2806 (Submission of an Information Disclosure Statement). But, because of the status of the Office Action associated with the application at the time of the IDS filing, this fee does not apply. As such, we should be refunded \$104.00.			

Requester's Information

Company or Firm Name (if applicable)		
Farjami & Farjami LLP		
Address Line 1	City	State/Region
26522 La Alameda Ave.	Mission Viejo	CA
Address Line 2 (if applicable)	Country	Zip/Postal Code
Suite 360	US	92691
Email Address (You will receive an acknowledgment of receipt only if you provide a valid email address)		Phone Number
egunderman@farjami.com		9492821000
Requester's Name		Registration Number (if applicable)
Evan C. Gunderman		
Signature		Date (mm/dd/yyyy)
/evan c. gunderman/		

Submit online via Patent Center (Patents customers who are registered users only): <https://patentcenter.uspto.gov>, or

Fax to: 571-273-6500, or

Mail to: Mail Stop 16, Director of the U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450



United States Patent and Trademark Office

Office of the Chief Financial Officer

October 28, 2024

Farjami & Farjami LLP
Attn: EVAN C. GUNDERMAN
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

Dear Sir/Madam,

The United States Patent and Trademark Office (USPTO) has reviewed your refund request for Reference Number **17577237** - Refund Request ID **REFND-20241023-70673**. Below is the current status of your refund request assigned to the following processing area: Office of Patent Examination Support Services

Fee code	Decision	Decision Reason(s)	Refund Amount
2806	Approved	No Fee Due	\$104.00

Generally, approved refunds will be issued in the form that the original payment was provided. You will receive a separate decision letter for any additional fee codes assigned to other processing areas, if applicable. Decisions may be subject to change if an error is identified.

For questions related to this decision, contact the Case Resolution Team at (571) 272-1720 or case.resolution@USPTO.GOV.

Thank you,
Refund Branch



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :Cathy Fowler

Refund Accounting Date:10/28/2024

Effective Date	Sale Item Reference Number	Refund Total
10/28/2024	17577237	\$104.00

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method	Account Number
I20240R001357137	2806	SUBMISSION- INFORMATION DISCLOSURE STMT	\$104.00	DA	500731



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :Cathy Fowler

Sale Adjustment Accounting Date:10/28/2024

Effective Date	Sale Accounting Date	Sale Item Reference Number
10/28/2024	10/28/2024	17577237

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20240R001357137	2806	SUBMISSION- INFORMATION DISCLOSURE STMT	\$104.00	DA



FARJAMI & FARJAMI LLP
An Intellectual Property Law Firm

EVAN C. GUNDERMAN
egunderman@farjami.com

October 11, 2024

Via Electronic Filing System (EFS)

Refunds Branch
Director of the United States Patent and Trademark Office
Attn: Deposit Accounts
2051 Jamieson Avenue, Suite 300
Alexandria, VA 22314

Re: Title: "Automated Device Provisioning and Activation"
Application Serial No.: 17/577,237
Amount of Charge: \$104.00; Fee Code: 2806; Date of Charge: 8/21/2024
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

Dear Refunds Branch:

Please refund \$104.00 to our Deposit Account, as we believe it was charged to our deposit account in error.

One June 19, 2024 we filed an Information Disclosure Statement in the above referenced application. The Application had a Non-Final Office Action attached to it which we had not yet filed a response to, but there was no Final Office Action or Notice of Allowance issued.

However, on August 21, 2024, we were charged \$104.00 to our Deposit Account under fee code 2806 (Submission of an Information Disclosure Statement). But, because of the status of the Office Action associated with the application at the time of the IDS filing, this fee does not apply. As such, we should be refunded \$104.00 charged to our Deposit Account on August 21, 2024.

Please advise when the refund of \$104.00 will be made by way of a credit to our Deposit Account. Thank you for your assistance in this matter.

Sincerely,
FARJAMI & FARJAMI LLP

/evan c. gunderman/

Evan C. Gunderman
Paralegal

26522 La Alameda Ave., Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	10/11/2024 06:26:05 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	67543440	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1C1C Let to PTO re Refund Request for 104 Charged on August 21 24.pdf	1	Refund Request	24 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C1C Let to PTO re Refund Request for 104 Charged on August 21 24.pdf	B6B6CFFF18DAD041B839B945505445C376849932C8BEF45DD76B2D147F7E61C3BD7365F0299147F63289155A1075143063EA64AB87DFF71A12F2AF262F2930E1

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

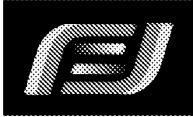
If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: September 13, 2024

To: United States Patent and Trademark Office
Examiner: Murillo Garcia, Fabricio R.; Art Unit: 2633

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 2

Message:

Enclosed, please find Request for Continued Examination regarding Consideration of Information Disclosure Statement as filed on September 5, 2024.

Credit card payment in the amount of **\$800.00** as the required Request for Continued Examination fee is hereby included with this filing.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

<h2 style="margin: 0;">REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL</h2> <p style="font-size: small; margin: 10px 0;">Subsection (b) of 35 U.S.C. § 132, effective on May 29, 2000, provides for continued examination of an utility or plant application filed on or after June 8, 1995. See The American Inventors Protection Act of 1999 (AIPA).</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Application Number</td> <td style="padding: 2px;">17/577,237</td> </tr> <tr> <td style="padding: 2px;">Filing Date</td> <td style="padding: 2px;">1/17/2022</td> </tr> <tr> <td style="padding: 2px;">First Named Inventor</td> <td style="padding: 2px;">Raleigh</td> </tr> <tr> <td style="padding: 2px;">Group Art Unit</td> <td style="padding: 2px;">2633</td> </tr> <tr> <td style="padding: 2px;">Examiner Name</td> <td style="padding: 2px;">Murillo Garcia, Fabricio R.</td> </tr> <tr> <td style="padding: 2px;">Attorney Docket Number</td> <td style="padding: 2px;">RALEP007C11C3C2C3C2C1C1 C1</td> </tr> </table>	Application Number	17/577,237	Filing Date	1/17/2022	First Named Inventor	Raleigh	Group Art Unit	2633	Examiner Name	Murillo Garcia, Fabricio R.	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1 C1
Application Number	17/577,237												
Filing Date	1/17/2022												
First Named Inventor	Raleigh												
Group Art Unit	2633												
Examiner Name	Murillo Garcia, Fabricio R.												
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1 C1												

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.

NOTE: 37 C.F.R. § 1.114 is effective on May 29, 2000. If the above-identified application was filed prior to May 29, 2000, applicant may wish to consider filing a continued prosecution application (CPA) under 37 C.F.R. § 1.53 (d) (PTO/SB/29) instead of a RCE to be eligible for the patent term adjustment provisions of the AIPA. See Changes to Application Examination and Provisional Application Practice, Final Rule, 65 Fed. Reg. 50092 (Aug. 16, 2000); Interim Rule, 65 Fed. Reg. 14865 (Mar. 20, 2000), 1233 Off. Gaz. Pat. Office 47 (Apr. 11, 2000), which established RCE practice.

1. **Submission required under 37 C.F.R. § 1.114**
 - a. ☒ Previously submitted
 - i. ☐ Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on _____
(Any unentered amendment(s) referred to above will be entered).
 - ii. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
 - iii. ☒ Other Information Disclosure Statement filed on September 5, 2024
 - b. ☐ Enclosed
 - i. ☐ Amendment/Reply
 - ii. ☐ Affidavit(s)/Declaration(s)
 - iii. ☐ Information Disclosure Statement (IDS)
 - iv. ☐ Other _____
2. **Miscellaneous**
 - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months, Fee under 37 C.F.R. § 1.17(i) required)
 - b. ☐ Other _____
3. **Fees** The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed.
 - a. ☒ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 50-0731
 - i. ☒ RCE fee required under 37 C.F.R. § 1.17(e)
 - ii. ☒ Extension of time fee (37 C.F.R. §§ 1.136 and 1.17)
 - iii. ☐ Other _____
 - b. ☐ Check in the amount of \$ _____ enclosed.
 - c. ☒ Payment to be charged by Credit Card in the amount of **\$800.00**.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print/Type)	Farshad Farjani, Esq.	Registration No. (Attorney/Agent)	41,014
Signature	/Farshad Farjami/	Date	September 13, 2024

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: **Mail Stop RCE**, Commissioner For Patents, P. O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office on:

Name (Print/Type)	Evan C. Gunderman	Date	September 13, 2024
Signature	/evan c. gunderman/		



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 09/13/2024 05:37:04 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	67173390	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C 1C1C1_RCE_Sept_13_24.pdf	2	-	68 KB
RALEP007C11C3C2C3C2 C1C1C1_RCE_Sept_13_24 -TRAN.LET.pdf	(1-1) 1	Transmittal Letter	31 KB
RALEP007C11C3C2C3C2 C1C1C1_RCE_Sept_13_24 -RCEX.pdf	(2-2) 1	Request for Continued Examination (RCE)	35 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
----------	-------------------------

RALEP007C11C3C2C3C2C1C 1C1_RCE_Sept_13_24.pdf	D29DB86416FE21B68C0C9B8BA6E0F6464850E44C320D079D6 420701DFDDB005242C10AA8639E8780BCA6FC2FA13CB5F20 F65CFFD8A02B0DE5063175173BB5E4A
RALEP007C11C3C2C3C2C1C 1C1_RCE_Sept_13_24- TRAN.LET.pdf	C55BADA7E68BA05B34BF440787E4953B598C168312000E2F4 91FE71FCEE9ECFFB03145CAFE0863943AFAC241F742EE690 508B00550254D5E2A042059AE5C2BBB
RALEP007C11C3C2C3C2C1C 1C1_RCE_Sept_13_24- RCEX.pdf	0C082BC1ED34545CFB0D743D74D7591DE2167A1AB73B8917 E4251BF09DD0A6826E8C0E2F9A38913996FAC9886A8B7FA6E 4F57DAD9CDA81583D43043FF396729B

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	09/13/2024 05:37:04 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	67173390	AUTHORIZED BY	Michael Farjami
CUSTOMER #	106963	FILING DATE	01/17/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Gregory G. Raleigh

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 5006	E20249CH38095209	Evan Gunderman

PRE-AUTHORIZED ACCOUNT	PRE-AUTHORIZED CATEGORY
500731	37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees); 37 CFR 1.21 (Miscellaneous fees and charges)

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2820	REQUEST FOR CONTINUED EXAMINATION (RCE)- 2ND AND SUBSEQUENT REQUEST (SEE 37 CFR 1.114)	800.00	1	800.00
TOTAL AMOUNT:				\$800.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850

7590 09/13/2024
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

EXAMINER

MURILLO GARCIA, FABRICIO R

ART UNIT	PAPER NUMBER
----------	--------------

2633

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

09/13/2024

ELECTRONIC

NOTICE OF NON-COMPLIANT INFORMATION DISCLOSURE STATEMENT

An Information Disclosure Statement (IDS) filed 09/05/2024 in the above-identified application fails to meet the requirements of 37 CFR 1.97(d) for the reason(s) specified below. Accordingly, the IDS will be placed in the file, but the information referred to therein has not been considered.

The IDS is not compliant with 37 CFR 1.97(d) because:

☒ The IDS lacks a statement as specified in 37 CFR 1.97(e).

☒ The IDS lacks the fee set forth in 37 CFR 1.17(p).

☐ The IDS was filed after the issue fee was paid. Applicant may wish to consider filing a petition to withdraw the application from issue under 37 CFR 1.313(c) to have the IDS considered. See MPEP 1308.

C. Garner, for
571-272-4200 or 1-888-786-0101
Application Assistance Unit
Office of Data Management

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	8,285,850		2012-10-09	Jones; Nathan et al.	
	2	5,987,611		1999-11-16	Freund; Gregor	
	3	6,947,723		2005-09-20	Gumani; Roger et al.	
	4	7,454,446		2008-11-18	Leung; Albert et al.	
	5	8,799,242		2014-08-05	Leonard; Glenda Ann et al.	
	6	7,860,964		2010-12-28	Brady; Mark et al.	
	7	5,481,735		1996-01-02	Mortensen; Craig et al.	
	8	5,764,693		1998-06-09	Taylor; Bryan et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070149252		2007-06-28	Jobs; Steven P. et al.	
	2	20060039354		2006-02-23	Rao; Goutham P. et al.	
	3	20060075090		2006-04-06	Bocking; Andrew D. et al.	
	4	20060019632		2006-01-26	Cunningham; Ivy et al.	
	5	20060203739		2006-09-14	Padmanabhan; Venkata N. et al.	
	6	20080026787		2008-01-31	Ibrahim; Brima et al.	
	7	20080122796		2008-05-29	Jobs; Steven P. et al.	
	8	20090217065		2009-08-27	Araujo, JR.; Nelson S.	
	9	20080002652		2008-01-03	Gupta; Dev V. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2633	
	Examiner Name		Murillo Garcia, Fabricio R.	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	10	20070117550		2007-05-24	Boris; Adam et al.	
--	----	-------------	--	------------	--------------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Complaint for Patent Infringement in Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2-23-cv-00641 (EDTX), Dec. 29, 2023	☐
	2	Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298	☐
	3	Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39	☐
	4	Agrawal, et. al., 2005. Policy-based management of networked computing systems. IEEE Communications Magazine, 43(10), pp. 69-75	☐
	5	Blake, et al., IETF RFC 2475, "An Architecture for Differentiated Services," December 1998, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2475 on July 29, 2023	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2633
	Examiner Name	Murillo Garcia, Fabricio R.
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

6	Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024	☐
7	Damianou, et al., 2001. The ponder policy specification language. In Policies for Distributed Systems and Networks: International Workshop, POLICY 2001 Bristol, UK, January 29–31, 2001 Proceedings (pp. 18-38). Springer Berlin Heidelberg	☐
8	Stone, G.N., et al., 2001. Network policy languages: a survey and a new approach, IEEE network, 15(1), pp.10-21	☐
9	Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39), IEEE	☐
10	Simplified Policy Language (CIM-SPL). Document Number DSP0231, version, 1	☐
11	Ponnappan, et al., 2002, June. A policy based QoS management system for the IntServ/DiffServ based Internet. In Proceedings Third International Workshop on Policies for Distributed Systems and Networks (pp. 159-168), IEEE	☐
12	Gonçalves, et al., 2009, October. A graphical user interface for policy composition in CIM-SPL. In 2009 International Conference on Ultra Modern Telecommunications & Workshops (pp. 1-7), IEEE.	☐
13	Liao, S.H., 2005. Expert system methodologies and applications—a decade review from 1995 to 2004. Expert systems with applications, 28(1), pp. 93-103	☐
14	van Beek, et. al., 2004, January. Adaptive streaming of high quality video over wireless LANs. In Visual Communications and Image Processing 2004 (Vol. 5308, pp. 647-660). SPIE.	☐
15	Reeder, et al., 2007. Usability challenges in security and privacy policy-authoring interfaces. In Human-Computer Interaction— INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II 11 (pp. 141-155). Springer Berlin Heidelberg.	☐
16	Mansour, et al., 2001. Jitter control in QoS networks.IEEE/ACM Transactions On Networking, 9(4), pp.492-502.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	17	IETF RFC 793, Transmission Control Protocol, September 1981, downloaded from the Internet on August 14, 2024	☐
	18	Prasad, et. al., 1998. An overview of CDMA evolution toward wideband CDMA. IEEE communications Surveys, 1(1), pp.2-29.	☐
	19	Excerpts, Garg, "An overview of wireless systems." Wireless Communications Networking, Morgan Kaufmann, 1st edition. ISBN 123735807 (2007).	☐
	20	Li, et al., 2003, December. "Dynamic priority reallocation scheme for quality of service in IEEE 802.11e WLANs." In Multimedia Computing and Networking 2004 (Vol. 5305, pp. 83-94). SPIE	☐
	21	PETITION FOR INTER PARTES REVIEW OF UNITED STATES PATENT NO. 8,588,110, filed on August 28, 2024	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2633
	Examiner Name	Murillo Garcia, Fabricio R.
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-09-05
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 09/05/2024 03:04:26 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	67058499	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 22

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C 1C1C1_IDS_Sept_5_24.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1738 KB
Warning: This is not a USPTO supplied IDS fillable form. Data in the form cannot be automatically loaded to other USPTO systems.			
Exhibit 1004 Complaint.pdf	26	Non Patent Literature	1137 KB
Exhibit 1021 Lobo A policy description language.pdf	8	Non Patent Literature	9350 KB
Exhibit 1022 Verma Policy- based management of content distribution networks.pdf	7	Non Patent Literature	6688 KB
Exhibit 1023 Agrawal Policy- based management of	10	Non Patent Literature	327 KB

networked computing
systems.pdf

Exhibit 1024 Blake IETF RFC 2475.pdf	36	Non Patent Literature	1678 KB
Exhibit 1025 Westerinen IETF RFC 3198.pdf	19	Non Patent Literature	1606 KB
Exhibit 1026 Damianou The ponder policy specification language.pdf	11	Non Patent Literature	1434 KB
Exhibit 1027 Stone Network policy languages.pdf	12	Non Patent Literature	1470 KB
Exhibit 1028 Agrawal.pdf	11	Non Patent Literature	231 KB
Exhibit 1029 Simplified Policy Language.pdf	55	Non Patent Literature	16610 KB
Exhibit 1030 Ponnappan A policy based QOS management system.pdf	11	Non Patent Literature	6139 KB
Exhibit 1031 Goncalves A graphical user interface for policy composition in CIM-SPLL.pdf	7	Non Patent Literature	1534 KB
Exhibit 1038 Liao Expert system methodologies and applications.pdf	11	Non Patent Literature	773 KB
Exhibit 1040 van Beek Adaptive streaming of high-quality video over wireless LANs.pdf	14	Non Patent Literature	11320 KB
Exhibit 1042 Reeder Usability challenges in security and privacy policy-authoring interfaces.pdf	15	Non Patent Literature	1257 KB
Exhibit 1043 Mansour Jitter control in QoS networks.pdf	26	Non Patent Literature	6929 KB
Exhibit 1046 IETF RFC 793.pdf	81	Non Patent Literature	2739 KB
Exhibit 1047 Prasad An overview of CDMA evolution toward wideband CDMA.pdf	28	Non Patent Literature	16343 KB

Exhibit 1049 Garg An overview of wireless systems.pdf	18	Non Patent Literature	901 KB
Exhibit 1050 Li Dynamic priority reallocation scheme.pdf	12	Non Patent Literature	10110 KB
Petition for Inter Partes Review.pdf	117	Non Patent Literature	6149 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C1C1_IDS_Sept_5_24.pdf	87896CDA522BA48B4E428018E40B55C1DE7826D26503321899E7A4A1013F1DB6F36FC36227202E1FE5BAE1E9FB098967436000DBBB478170CEA11F5A600F772D
Exhibit 1004 Complaint.pdf	B3CF3BC2890D9CB2C66858DEBECBC84F21E780878708563FC6FDC6569365295EE8BE1757051EB24D2889CA17D12520A933B94C978409AF202C3D46325414C5E2
Exhibit 1021 Lobo A policy description language.pdf	933BE30260D181934EC0A7C1A4F8FAEB09B804968A3333848689E07EE93CBB18B5E0A54272438049460F6F821DABE4FCA20E753BC8BD644C85E42A27011FA5C6
Exhibit 1022 Verma Policy-based management of content distribution networks.pdf	EF3F415057540A9EB327A7CA4D3BC661072A803B551F6C0976BE546930068D86EE679FCAE0B57663909BACCC91C1EF953357BFDF7DA1EB7B727822643954210F
Exhibit 1023 Agrawal Policy-based management of networked computing systems.pdf	9C874F332369A32AB3CAA7DFFC59811A6025198E53A59F7E24B92A650F6BE2E1CB94B336C4299ED01B70927560BECCC768ABAC22E0B4A0BB8D1CB2320BCDE996
Exhibit 1024 Blake IETF RFC 2475.pdf	BFCAB3AA8EB47A86571F2F10CBB74AB42AA163FC1DA45DBC93550165754854988DC03BF368B1D2D83AF1BE6806DB39C55A6FBCC19B12B79BD71FCEF7F2A9478
Exhibit 1025 Westerinen IETF RFC 3198.pdf	E26A20E16C2EF9CD10BF9AC9055127ECC78B76128CC028A4809315921B2FFEB2BAAB9B54968E4BB6662076AF1CBE07592306B349D50C36EA349839221CAF6F55
Exhibit 1026 Damianou The ponder policy specification language.pdf	A686ABD13E21E88C172612F4B5BC61A7E3FC669FEC0211628476F1A248468868A81FBC2D2986B0E3BBC7DE6F4B70BCFC169F5542BC2EF3902AB67F2EABB3CFF4
Exhibit 1027 Stone Network policy languages.pdf	74D366F7AFD9CEC1D522B870D4B7871287811BECB260A2745A3731EB1A266D2F2C963140E2184DEAD82D8F0B490108346AD87C447CB38BA232FBAD516894D3EC

Exhibit 1028 Agrawal.pdf	0AA06F2AFA7837E7B83CCADCC0B142AC41F6EB8F4C1A3848 840AF82F8294A09607BF4A075CD43EADDEE432D1FEC4A6D3 0D29BA4CBB3194CF045A834CC3C58646
Exhibit 1029 Simplified Policy Language.pdf	2C4FCBF654C1C5F69CE1392A608F2406EEE309F78CD86BB7 9C2010B4D1C894EA15C56934C2C60A05723ACC802DFCF9FC 51CA8FF23E924BFC4C90727BA932D786
Exhibit 1030 Ponnappan A policy based QOS management system.pdf	8DFF3C6A812997C0BE62BAB922BA44E56759FCF2D3D14C2F 572C45A464B3170568CB31448B7579EC008580C6440F213D7F D3C91ADB1AEB671C54A4DD38510506
Exhibit 1031 Goncalves A graphical user interface for policy composition in CIM-SPLL.pdf	4A934DE29126A211A93E3D717B671A08DE5814D7370B6DAFA 0BABA6C63B02E408B66D080491B9640898C0215F62B924A7B C7600AEEF3A5A4199BDFB083AE7541
Exhibit 1038 Liao Expert system methodologies and applications.pdf	A0C397FD551AAB0386EA06715C7972216B1C7407C5066A068 CF825442F6051071B74CED059446511D205AD92D491EBC025 12E59F3F01F619EE673621B6CB3B3A
Exhibit 1040 van Beek Adaptive streaming of high-quality video over wireless LANs.pdf	BA45D0BBF4E5969719537087C2E6EBE7C966166639129A1034 9C170E1D8F9BD143EBB12B965D18E3801AFAA1EFC8C1F670 7C474B787CC6808F0ADE39A4613920
Exhibit 1042 Reeder Usability challenges in security and privacy policy-authoring interfaces.pdf	CF7DECFFFD3CE4B6079D095E4F4DBE0DA39B6F94597F4575 B52705003A94915E7429056589A3B3D7979754B43B2FF53E9A 82D66444CF36F48154AFBC56C4DB6F
Exhibit 1043 Mansour Jitter control in QoS networks.pdf	F5271E9AA5124CAF96C067451582FCA8DFC59BB3EFAD378A 17C01EB3D123A3F80E885E608BFC5D0337DA1B89BAF9CE98 82C337DC961F675D3656FE9B4909945D
Exhibit 1046 IETF RFC 793.pdf	CE6426FAFA67E220945308252532ACAB72CD5D047F69BFD12 6A9D60ACC9DEC9872742F78A032D7544933159BD97EEA305A AE3A9882EF7198439FE710B1489F3B
Exhibit 1047 Prasad An overview of CDMA evolution toward wideband CDMA.pdf	14113DB4CA3BF961F9F6D1F30436EA1C62EEB43B521551219 03CDB586D3761B34621C5EC9AFB14920BFCF4B43EEE980E8 A1C96416117D39011D104B5B889751C
Exhibit 1049 Garg An overview of wireless systems.pdf	286C0C4CB0A75CAB666111F3D4DF7F05531F2B04309927E3A 27EBFE64BB3214046B5435A2A514316DFFBC2048EB126B4E9 54B810BD767CA904ADDF4A0C46DE98
Exhibit 1050 Li Dynamic priority reallocation scheme.pdf	82927FBA9BE7E4A0316697FABC351EE176223BB1D48AB8FA DFEB273A3D3319FD40A63233DA7DB85382E16E310C1347EF BA499231167A133204E5D6C993861BBB
Petition for Inter Partes Review.pdf	E0D4200C51DBAF2F4CE6FE01EC71A36630D6BE8BB54E04A1 D4F8C525B049354691E4FCFB0FC85F11A501D95ECF650EBE1 C0ABC5CBAD8E6C475184E1E150CDA1C

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

AUTOMATED DEVICE PROVISIONING AND ACTIVATION

BACKGROUND OF THE INVENTION

[0001] With the advent of mass market digital communications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), and Wi-Fi (Wireless Fidelity) wireless networks increasingly becoming user capacity constrained. Although wireless network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0002] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0004] FIG. 1 illustrates a simplified (e.g., “flattened”) network architecture in accordance with some embodiments.

[0005] FIG. 2 illustrates another simplified (e.g., “flattened”) network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments.

[0006] FIG. 3 illustrates another simplified (e.g., “flattened”) network architecture including two central providers in accordance with some embodiments.

[0007] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments.

[0008] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments.

[0009] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments.

[0010] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments.

[0011] FIG. 8 illustrates another simplified (e.g., “flattened”) network architecture including multiple wireless access networks (e.g., 3G and 4G Wireless Wide Area Networks (WWANs)) and multiple wire line networks (e.g., Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks) in accordance with some embodiments.

[0012] FIG. 9 illustrates a hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0013] FIG. 10 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0014] FIG. 11 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0015] FIG. 12 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0016] FIG. 13 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0017] FIG. 14 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0018] FIGS. 15A through 15F illustrate hardware diagrams of a device that include a service processor and a bus structure extension using intermediate modem or networking device combinations in accordance with various embodiments.

[0019] FIG. 16 is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

[0020] FIG. 17 is another functional diagram illustrating the device based service processor and the service controller in accordance with some embodiments.

[0021] FIG. 18 is another functional diagram illustrating the device based service processor and the service controller in which the service processor controls the policy implementation for multiple access network modems and technologies in accordance with some embodiments.

[0022] FIG. 19 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0023] FIG. 20 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0024] FIG. 21 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0025] FIGS. 22A and 22B provide tables summarizing various service processor agents (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0026] FIG. 23 provides a table summarizing various service controller server elements (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0027] FIG. 24 is a functional diagram illustrating the service control device link of the service processor and the service control service link of the service controller in accordance with some embodiments.

[0028] FIG. 25 is a functional diagram illustrating framing structure of a service processor communication frame and a service controller communication frame in accordance with some embodiments.

[0029] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters in accordance with some embodiments.

[0030] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments.

[0031] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments.

[0032] FIG. 29 is a functional diagram illustrating a device communications stack that allows for implementing verifiable traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0033] FIG. 30 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0034] FIG. 31 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0035] FIG. 32 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0036] FIG. 33 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0037] FIG. 34 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0038] FIG. 35 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0039] FIG. 36 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0040] FIG. 37 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0041] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments.

[0042] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0043] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0044] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments.

[0045] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments.

[0046] FIGS. 43A through 43B are flow diagrams illustrating a flow diagram for a service processor authorization sequence as shown in FIG. 43A and a flow diagram for a service controller authorization sequence as shown in FIG. 43B in accordance with some embodiments.

[0047] FIGS. 44A through 44B are flow diagrams illustrating a flow diagram for a service processor activation sequence as shown in FIG. 44A and a flow diagram for a service controller activation sequence as shown in FIG. 44B in accordance with some embodiments.

[0048] FIGS. 45A through 45B are flow diagrams illustrating a flow diagram for a service processor access control sequence as shown in FIG. 45A and a flow diagram for a service controller access control sequence as shown in FIG. 45B in accordance with some embodiments.

[0049] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0050] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0051] FIG. 48 illustrates a network architecture including a service controller device control system and a service controller analysis and management system in accordance with some embodiments.

[0052] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments.

[0053] FIG. 50 illustrates a network architecture including a billing to service controller interface for accommodating minimum changes in existing central billing, AAA and/or other network components in accordance with some embodiments.

[0054] FIG. 51 illustrates a network architecture for locating service controller device control functions with AAA and network service usage functions in accordance with some embodiments.

[0055] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments.

[0056] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments.

[0057] FIG. 54 illustrates a network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0058] FIG. 55 illustrates another network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0059] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0060] FIG. 57 illustrates a network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0061] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0062] FIG. 59 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0063] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0064] FIG. 61 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0065] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0066] FIG. 63 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0067] FIG. 64 illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments.

DETAILED DESCRIPTION

[0068] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term “processor” refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0069] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0070] With the development and increasing proliferation of mass market digital communications and content distribution, communication network capacity gains are being outpaced by growing digital networking demand. For example, some industry experts project average wireless device usage of four devices per subscriber, with a mixture of general purpose devices like smart phones and computers along with special purpose devices like music players, electronic readers, connected (e.g., networked) cameras and connected gaming devices. In

addition, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience if not efficiently managed. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

[0071] There is a need for a communication system and method that provides for flexible service plans and management of user network services to provide consumer choice of more refined service plan offerings and efficient management of network capacity.

[0072] Also, it is becoming increasingly important to more deeply manage the level of services delivered to networked devices to provide cost effective services that match growing digital networking usage patterns. For example, access providers can move away from only billing for basic access and move toward billing for higher level service delivery with example services including rich Internet access and email, application based billing, content distribution, entertainment activities, information or content subscription or gaming. In addition, a growing number of new special purpose and general purpose networked devices are fueling demand for new service plans, for example, tailored to the new device usage models (e.g., a special service plan for an e-book reader device).

[0073] As network capabilities grow and new networked device offerings grow, access network service providers will realize increasing value in opening up their networks to allow innovation and expanded offerings for network service consumers. However, opening up the networks to provide efficient third party definition of alternative service and billing models requires more flexible service and billing policy management solutions. For example, machine to machine applications such as telemetry, surveillance, shipment tracking and two way power control systems are example new applications that would require new offerings to make such available to network service customers. The need to customize service offerings for these new applications requires more efficient methods for defining, testing and launching new services with more refined control of service functions and service costs. In some embodiments, this means billing for different types of service elements, such as total traffic, content downloads, application usage, information or content subscription services, people or asset tracking services, real time machine to machine information or electronic commerce transactions.

[0074] In some embodiments, network user capacity is increased and user service costs are reduced by managing and billing for service consumption in a more refined manner (e.g., to satisfy network neutrality requirements). By managing service consumption in a user friendly manner, the overall service capacity required to satisfy the user device needs can be tailored more closely to the needs of a given user thereby reducing user service costs and increasing service provider profits. For example, managing service usage while maintaining user satisfaction includes service usage policy implementation and policy management to identify, manage and bill for service usage categories, such as total traffic consumption, content downloads, application usage, information or content subscription services, electronic commerce transactions, people or asset tracking services or machine to machine networking services. As described herein, service activity is used to refer to any service usage or traffic usage that can be associated with, for example, an application; a network communication end point, such as an address, uniform resource locator (URL) or other identifier with which the device is communicating; a traffic content type; a transaction where content or other material, information or goods are transacted, purchased, reserved, ordered or exchanged; a download, upload or file transfer; email, text, SMS, IMS or other messaging activity or usage; VOIP services; video services; a device usage event that generates a billing event; service usage associated with a bill by account activity (also referred to as billing by account) as described herein; device location; device service usage patterns, device user interface (UI) discovery patterns, content usage patterns or other characterizations of device usage; or other categories of user or device activity that can be identified, monitored, recorded, reported, controlled or processed in accordance with a set of verifiable service control policies. As will be apparent to one of ordinary skill in the art in view of the embodiments described herein, some embodiments identify various service activities for the purpose of decomposing overall service usage into finer sub-categories of activities that can be verifiably monitored, categorized, cataloged, reported, controlled, monetized and used for end user notification in a manner that results in superior optimization of the service capabilities for various levels of service cost or for various types of devices or groups. In some embodiments, it will be apparent to one of ordinary skill in the art that the terms service activity or service usage are associated with categorizing and possibly monitoring or controlling data traffic, application usage, communication with certain network end points, or transactions, and it will also be apparent that in some embodiments the term service activity is

intended to include one or more of the broader aspects listed above. The shortened term service usage can be used interchangeably with service activity, but neither term is intended in general to exclude any aspect of the other. In some cases, where the terms service usage or service activity are used, more specific descriptors such as traffic usage, application usage, website usage, and other service usage examples are also used to provide more specific examples or focus in on a particular element of the more encompassing terms.

[0075] In some embodiments, employing this level of service categorization and control is accomplished in a manner that satisfies user preferences. In some embodiments, employing this level of service categorization and control is accomplished in a manner that also satisfies government rules or regulations regarding open access, for example, network neutrality requirements. In some embodiments, service management solutions that also collect and/or report user or device service usage or service activity behavior to determine how best to meet the user's simultaneous desires for service quality and lower service costs are disclosed. For example, such monitoring and reporting are accomplished in a manner that includes approval by the user and in a manner that also protects the privacy of user information and service usage behavior or service activity history.

[0076] In some embodiments, a system and method is disclosed for increasing network user capacity for wireless networks in the face of increasing service demand per user by providing for a greater number of base stations, also sometimes referred to as access points, base terminals, terminal nodes or other well known acronyms, to be more easily and/or more cost effectively deployed. For example, to simplify the process of deploying base stations, the installation complexity and the network infrastructure required for the base station to obtain backhaul service to the various networks that users desire to connect with are reduced.

[0077] In some embodiments, dense base station deployments are simplified by reducing the requirement to aggregate or concentrate the base station traffic through a specific dedicated core network infrastructure, so that the base stations connect to the desired user networks through a more diverse set of local loop, back bone and core routing options. This approach also reduces network infrastructure equipment, installation and maintenance costs. In some embodiments, this is accomplished by distributing the network traffic policy implementation and

control away from the core network by providing for more control for service policy implementation and management on the end user device and, in some embodiments, in the end user device with respect to certain service policies and the network (e.g., control plane servers) with respect to other service policies. For example, this approach facilitates connecting the base stations directly to the local loop Internet with a minimum of specific dedicated networking infrastructure.

[0078] In some embodiments, service and transaction billing event capture and logging are distributed to the device. For example, providing service and transaction billing event capture and logging at the device provides a greater capability to monitor, classify and control deeper aspects of service usage or service activity at the device as compared to the relatively less capability for the same in the network infrastructure (e.g., for certain traffic flows, such as encrypted traffic flows). Furthermore, billing at the device provides for very specialized with many different billing and service plans for different device and service usage or service activity scenario combinations without the problem of attempting to propagate and manage many different deep packet inspection (DPI) and traffic shaping profiles in the networking equipment infrastructure. For example, service billing at the device can provide for more sophisticated, more specialized and more scalable billing and service plans.

[0079] Another form of billing that needs improvement is electronic commerce transaction billing with device assisted central billing. Today, most central billing and content distribution models require either centralized content distribution maintained by the central service provider or central billing authority, or a centralized ecommerce website or portal traffic aggregation system controlled by the central service provider or central billing provider, or both. In such systems, content and transaction providers such as media providers, application developers, entertainment providers, transaction website providers and others must adapt their mainstream electronic offering and commerce systems, such as shopping experience websites, to fit within the various proprietary customized infrastructure and content storage solutions for ecommerce markets, such as BREW® (Binary Runtime Environment for Wireless from Qualcomm® Inc.), Symbian OS (from Symbian Software Ltd) and Apple iPhone 3G App Store (from Apple Inc.). This approach requires a large amount of unnecessary custom interface development and stifles open market creativity for HTTP, WAP or portal/widget based shopping

destinations and experiences. As disclosed below, a superior approach includes device based transaction billing for an open ecosystem in which a central billing provider provides users and ecommerce transaction providers with a central billing solution and experience that does not require extensive custom development or ecommerce infrastructure interfacing.

[0080] In some embodiments, products that incorporate device assisted service policy implementation, network services and service profiles (e.g., a service profile includes a set of one or more service policy settings for the device for a service on the network) are disclosed, as described below. For example, aspects of the service policy (e.g., a set of policies/policy settings for the device for network services, typically referring to lower level settings, such as access control settings, traffic control settings, billing system settings, user notification settings, user privacy settings, user preference settings, authentication settings and admission control settings) that are moved out of the core network and into the end user device include, for example, certain lower level service policy implementations, service usage or service activity monitoring and reporting including, for example, privacy filtering, customer resource management monitoring and reporting including, for example, privacy filtering, adaptive service policy control, service network access control services, service network authentication services, service network admission control services, service billing, transaction billing, simplified service activation and sign up, user service usage or service activity notification and service preference feedback and other service capabilities.

[0081] As discussed below, product designs that move certain aspects of one or more of these service profile or service policy implementation elements into the device provide several advantageous solutions to the needs described above. For example, benefits of certain embodiments include the ability to manage or bill for a richer and more varied set of network services, better manage overall network capacity, better manage end user access costs, simplify user or new device service activation, simplify development and deployment of new devices with new service plans (e.g., service profile and billing/costs information associated with that service profile), equip central service providers with more effective open access networks for new third party solutions, simplify the equipment and processes necessary to deploy wireless base stations and simplify the core networking equipment required to deploy certain access networks.

[0082] As discussed below, there are two network types that are discussed: a central provider network and a service provider network. The central provider network generally refers to the access network required to connect the device to other networks. The central provider network generally includes the physical layer, the Media Access Control (MAC) and the various networking functions that can be implemented to perform authentication, authorization and access control, and to route traffic to a network that connects to the control plane servers, as discussed below. The service provider network generally refers to the network that includes the control plane servers. In some embodiments, a central provider network and a service provider network are the same, and in some embodiments, they are different. In some embodiments, the owner or manager of the central provider network and the owner or manager of the service provider network are the same, and in some embodiments, they are different.

[0083] In some embodiments, control of the device service policies is accomplished with a set of service control plane servers that reside in the access network or any network that can be reached by the device. This server based control plane architecture provides for a highly efficient means of enabling third party control of services and billing, such as for central carrier open development programs or Mobile Virtual Network Operator (MVNO) relationships. As device processing and memory capacity expands, moving to this distributed service policy processing architecture also becomes more efficient and economical. In some embodiments, several aspects of user privacy and desired network neutrality are provided by enabling user control of certain aspects of device based service usage or service activity reporting, traffic reporting, service policy control and customer resource management (CRM) reporting.

[0084] In many access networks, such as wireless access networks, bandwidth capacity is a valuable resource in the face of the increasing popularity of devices, applications and content types that consume more bandwidth. To maintain reasonable service profit margins, a typical present service provider practice is to charge enough per user for access to make service plans profitable for the higher bandwidth users. However, this is not an optimal situation for users who desire to pay less for lower bandwidth service usage or service activity scenarios.

[0085] Accordingly, in some embodiments, a range of service plan pricing can be enabled that also maintains service profitability for the service provider, for example, by

providing a more refined set of management and control capabilities for service profiles. For example, this approach generally leads to service management or traffic shaping where certain aspects of a service are controlled down based on service policies to lower levels of quality of service. Generally, there are three problems that arise when these techniques are implemented. The first problem is maintaining user privacy preferences in the reporting of service usage or service activity required to set, manage or verify service policy implementation. This problem is solved in a variety of ways by the embodiments described below with a combination of user notification, preference feedback and approval for the level of traffic information the user is comfortable or approves and the ability to filter service usage or service activity, in some embodiments, specifically traffic usage or CRM reports so that only the level of information the user prefers to share is communicated. The second problem is satisfying network neutrality requirements in the way that traffic is shaped or services are managed. This problem is solved in a variety of ways as described in the embodiments described below by empowering the user to make the choices on how service usage, service activity, traffic usage or CRM data is managed down to control costs, including embodiments on user notification and service policy preference feedback. By allowing the user to decide how they want to spend and manage their service allowance or resources, a more neutral or completely neutral approach to network usage can be maintained by the service provider. The third problem is to help the user have an acceptable and enjoyable service experience for the lower cost plans that will result in much wider scale adoption of connected devices and applications but are more constrained on service activity usage or options or bandwidth or traffic usage. As lower cost service plans are offered, including plans where the basic connection service may be free, these service plans will require service provider cost controls to maintain profitability or preserve network capacity that result in lower limits on service usage or service activity. These lower service usage or service activity limit plans will result in more users who are likely run over service usage limits and either experience service shutdown or service cost overages unless they are provided with more capable means for assistance on how to use and control usage for the lower cost services. This problem is solved in a variety of ways with a rich collection of embodiments on user notification, service usage and cost projection, user notification policy feedback, user service policy preference feedback, and adaptive traffic shaping or service policy implementation. As described herein, some embodiments allow a wide range of flexible and verifiable service plan and service profile

implementations ranging from examples such as free ambient services that are perhaps sponsored by transaction revenues and/or bill by account sponsored service partner revenues, to intermediately priced plans for basic access services for mass market user devices or machine to machine communication devices, to more expensive plans with very high levels of service usage or service activity limits or no limits at all. Several bill by account embodiments also provide for the cataloging of service usage that is not a direct benefit to end users but is needed for basic maintenance of the device control channels and access network connection, so that the maintenance traffic service cost can be removed from the user billing or billed to non-user accounts used to track or account for such service costs. These embodiments and others result in a service usage or service activity control capability that provides more attractive device and service alternatives to end users while maintaining profitability for service providers and their partners.

[0086] In some embodiments, the above described various embodiments for device based service policy and/or service profile communications control are implemented using network based service control, for example, for satisfying various network neutrality and/or privacy requirements, based on indication(s) received from the device (e.g., user input provided using the device UI using the service processor) and network based service control (e.g., using a DPI service monitor or DPC policy implementation and/or other network elements).

[0087] In some embodiments, a virtual network overlay includes a device service processor, a network service controller and a control plane communication link to manage various aspects of device based network service policy implementation. In some embodiments, the virtual network overlay networking solution is applied to an existing hierarchical network (e.g., for wireless services), and in some embodiments, is applied to simplify or flatten the network architecture as will be further described below. In some embodiments, the large majority of the complex data path network processing required to implement the richer service management objectives of existing hierarchical networks (e.g., for wireless services) are moved into the device, leaving less data path processing required in the edge network and in some cases even less in the core network. Because the control plane traffic between the service control servers and the device agents that implement service policies can be several orders of magnitude slower than the data plane traffic, service control server network placement and back-haul

infrastructure is much less performance sensitive than the data plane network. In some embodiments, as described further below, this architecture can be overlaid onto all the important existing access network architectures used today. In some embodiments, this architecture can be employed to greatly simplify core access network routing and data plane traffic forwarding and management. For example, in the case of wireless networks, the incorporation of device assisted service policy implementation architectures can result in base stations that directly connect to the Internet local loop and the data traffic does not need to be concentrated into a dedicated core network. This results, for example, in a large reduction in backhaul cost, core network cost and maintenance cost. These cost savings can be re-deployed to purchase and install more base stations with smaller cells, which results in higher data capacity for the access network leading to better user experience, more useful applications and lower service costs. This flattened networking architecture also results in latency reduction as fewer routes are needed to move traffic through the Internet. In some embodiments, the present invention provides the necessary teaching to enable this powerful transformation of centralized network service architectures to a more distributed device based service architectures.

[0088] Device based billing can be compromised, hacked and/or spoofed in many different ways. Merely determining that billing reports are being received from the device, that the device agent software is present and properly configured (e.g., the billing agent is present and properly configured) is insufficient and easily spoofed (e.g., by spoofing the agent itself, providing spoofed billing reports using a spoofed billing agent or providing spoofed agent configurations). Accordingly, in some embodiments, verifiable device assisted and/or network based service policy implementation is provided. For example, verifiable service usage and/or service usage billing can be provided as described herein with respect to various embodiments.

[0089] While much of the below discussion and embodiments described below focus on paid service networks, those of ordinary skill in the art will appreciate that many of the embodiments also apply to other networks, such as enterprise networks. For example, the same device assisted network services that create access control services, ambient activation services and other service profiles can be used by corporate IT managers to create a controlled cost service policy network for corporate mobile devices. As another example, embodiments described below for providing end user service control can also allow a service provider to offer

parental controls by providing parents with access to a website with a web page that controls the policy settings for the access control networking service for a child's device.

Network Architecture for Device Assisted/Based Service Control

[0090] FIG. 1 illustrates a simplified (e.g., “flattened”) network architecture in accordance with some embodiments. As shown, this provides for a simplified service infrastructure that exemplifies a simplified and “flattened” network architecture in accordance with some embodiments that is advantageous for wireless network architectures. This also reduces the need for complex data path protocol interaction between the base station and network infrastructure. For example, in contrast to a complex edge and core network infrastructure connecting base stations to the central service provider network, as shown the base stations 125 are connected directly to the Internet 120 via firewalls 124 (in some embodiments, the base stations 125 include the firewall functionality 124). Accordingly, in some embodiments, a central provider network is no longer required to route, forward, inspect or manipulate data plane traffic, because data plane traffic policy implementation is conducted in the device 100 by the service processor 115. However, it is still an option, in some embodiments, to bring data plane traffic in from the base stations 125 to a central provider network using either open or secure Internet routing if desired. Base station control plane communication for access network AAA (Authentication, Authorization, and Accounting) server 121, DNS/DHCP (Domain Name System/Dynamic Host Configuration Protocol) server 126, mobile wireless center 132 (sometimes referenced to in part as a home location register (HLR) or other acronym) or other necessary functions are accomplished, for example, with a secure IP tunnel or TCP connection between the central provider network and the base stations. The base station 125 is used to refer to multiple base station embodiments where the base station itself is directly connected to the RAN, or where the base station connects to a base station controller or base station aggregator function that in turn connects to the RAN, and all such configurations are collectively referred to herein as base station 125 in FIG. 1 and most figures that follow that reference base station 125 as described below.

[0091] As shown, the central provider access network is both 3G and 4G capable, the devices 100 can be either 3G, 4G or multi-mode 3G and 4G. Those of ordinary skill in the art

will also appreciate that in the more general case, the network could be 2G, 3G and 4G capable, or the device could be 2G, 3G and 4G capable with all or a subset of Global System for Mobile (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA) 1X, High Speed Packet Access (HSPA), Evolution Data Optimized (EVDO), Long Term Evolution (LTE) and WiMax modem capability. If the devices are single mode, then the 3G devices 100 will be activated with a service profile applied to service processor 115 that is consistent with the 3G network capacity and speed, and the 4G devices will be activated with service profiles applied to service processor 115 that are consistent with 4G network capacity and speed. In both cases, the same service controller 122 manages services for both sets of devices in accordance with some embodiments. If the devices are multimode, then the service processor 115 can be activated with a dual mode service profile capability in which the service profile for 3G offers a similar rich set of services as the service profile for 4G but with, for example, scaled back bandwidth. For example, this approach allows central providers to offer a richer set of service offerings with 3G and then migrate the same set of service offerings to 4G but with higher performance. In particular, this approach allows 3G to 4G rich service migration to occur, for example, with the only change being the increased bandwidth settings in the service profiles that will be available in 4G at the same cost as 3G with lower service profile bandwidth settings.

[0092] In some embodiments, if the devices are multimode, a network selection policy implementation within service processor 115 is provided, or in some embodiments, a network selection policy is driven by policy decisions made in service controller 122 based on service availability reports received from service processor 115. The network selection policy allows the selection of the network that corresponds to the most desirable service profile to meet the user's service preferences. For example, if the user specifies, within the framework of the service notification and user preference feedback embodiments described below, that maximum performance is the most important factor in selecting which access network to connect to, then the best profile is likely to be the 4G network as 4G is typically faster, except perhaps, for example, if the device 100 is closer to the 3G base station so that there is a much stronger signal or if the 4G network is much more heavily loaded than the 3G network. On the other hand, if the user preference set specifies cost as the most important factor, then depending on the central provider service costs the 3G network may prove to be the most desirable service profile. This is

a simple example and many other selection criteria are possible in the network selection embodiment as discussed further below.

Network Based Service Usage Monitoring for Verification and Other Purposes

[0093] In some embodiments, if the base station data plane traffic is transmitted via the Internet 120 as discussed above, then IPDRs (Internet Protocol Detail Records, also sometimes and interchangeably referred to herein as Charging Data Records or CDRs, which as used herein refer to any network measure of service usage or service activity for voice and/or data traffic (e.g., IPDRs can include a time stamp, a device ID, and various levels of network measures of service usage for the device associated with that device ID, such as perhaps total traffic usage, network destination, time of day or device location)) are generated by and collected from the access network equipment. Depending on the specific network configuration, as discussed herein, for a WWAN network the IPDRs can be generated by one or more of the following: base station 125, RAN or transport gateways and AAA 121. In some access network embodiments, the IPDRs are transmitted to equipment functions that aggregated the IPDRs for the purpose of service billing and other functions. Aggregation can occur in the AAA, the transport gateways or other functions including the billing system 123. As discussed below, it is often the case that the IPDRs is assumed to be obtained from the AAA server 121 and/or a service usage data store 118 (e.g., a real-time service usage collection stored in a database or a delayed feed service usage collection stored in a database), or some other network function. However, this does not imply that the IPDRs may not be obtained from a variety of other network functions, and in some embodiments, the IPDRs are obtained from other network functions as disclosed herein. In some embodiments, existing IPDR sources are utilized to obtain network based service usage measures for multiple purposes including but not limited to service policy or profile implementation verification, triggering service verification error responds actions, and service notification synchronization. Certain types of IPDRs can be based on, or based in part on, what are sometimes referred to as CDRs (Charging Data Records, which can track charges for voice and data usage) or modifications of CDRs. Although the capability to monitor, categorize, catalog, report and control service usage or service activity is in general higher on the device than it is in the network, and, as described herein, device based service monitoring or control assistance is in some ways desirable as compared to network based implementations, as described herein many

embodiments take advantage of network based service monitoring or control to augment device assisted service monitoring or control and vice versa. For example, even though many embodiments work very well with minimal IPDR service usage or service activity information that is already available in a network, deeper levels of IPDR packet inspection information in general enable deeper levels of service monitoring or service control verification, which can be desirable in some embodiments. As another example, deeper levels of network capability to control service usage or service activity can provide for more sophisticated error handling in some embodiments, for example, providing for more options of the Switched Port Analyzer (SPAN) and network quarantine embodiments as described herein. As another example, in some embodiments it is advantageous to take advantage of network based service monitoring or control for those service aspects the network is capable of supporting, while using device assisted service monitoring or control for the service aspects advantageously implemented on the device.

[0094] In some embodiments, where base station data plane traffic is backhauled and concentrated in a central provider core network 110, then the IPDRs can originate in the base stations or a router or gateway in the central provider network 110, and the IPDRs are collected at the AAA server 121 and stored in the service usage data store 118. In some embodiments, the central billing system 123 collects the IPDRs from the AAA server 121 for service billing accounting purposes. In some embodiments, a central billing system 123 collects the IPDRs directly from the initial IPDR source or some other aggregator. In some embodiments, outside partners like MVNOs gain access to the IPDRs from the central billing system 123. As discussed below, it is assumed that the IPDRs are obtained from the AAA server 121, and it is understood that the source of the IPDRs is interchangeable in the embodiments.

[0095] In some embodiments, the IPDR information is used by the service processor 115, the service controller 122 and/or other network apparatus or device apparatus to implement service control verification is provided as described below. In some embodiments, an IPDR feed (e.g., also referred to as a charging data record (CDR)) flows between network elements. For example, an IPDR feed can flow from the RAN gateway 410 (e.g., SGSN 410, BSC packet control 510 or RNC 512) and the transport gateway 420 (e.g., GGSN or PDSN). In other embodiments, the IPDRs originate and flow from the base station 125 or some other

component/element in the network. In some embodiments, one or more of these IPDR feeds is transmitted to an IPDR aggregation function (e.g., also referred to as a charging gateway). For example, this aggregation function can be located in the AAA 121, in the mobile wireless center 132 (and/or in the home location register (HLR) or other similar function referred to by other common industry names), in the transport gateway 420, or in some other network element. This aggregation function collects the IPDR feeds into a database with an entry for each device 100. In some embodiments, an intermediate aggregation function is provided that feeds a higher level aggregation function, for example, the transport gateway 420 can receive IPDR feeds from the RAN gateway 410 or the base station 125 before sending them to another aggregation function. At some point in time (e.g., at the end of a specified time period, at the end of a device network connection session and/or at a specified time of day), the IPDR aggregation function sends summary information or detailed information of the IPDRs for a given device or group of devices to the billing system for billing and/or reconciliation. In some embodiments, in which the IPDR aggregation feed to the billing system is frequent enough for one or more of the IPDR information purposes described herein, the IPDR feed for the service controller 122 is derived from the aggregated feed, either by having the billing system 123 transmit it to the service controller 122, or by copying it from the IPDR aggregation function.

[0096] In some embodiments, the IPDR feed is obtained from the network function that is generating or aggregating the IPDR feed as described herein. In some embodiments, the IPDR feed is copied from the aggregation function in a manner that does not interrupt the operation of the network. For example, a switch based port analysis function can be used to copy the traffic to a traffic analysis or server element that filters out the IPDR traffic and records it to a data base that is then either pushed to the service controller 122 (or any other network element that uses IPDR information as described herein), or is queried by the service controller 122 (or any other function that uses the IPDR information as described herein). In some embodiments, if the aggregated IPDR information transmitted to the billing system is delayed from real-time traffic usage events by an amount of time that is, for example, too long for desired operation, or for any other reason that makes it less desirable to obtain the IPDR information from the same aggregated feed used for the billing system 123, the IPDR information can be collected from one or more of the sources discussed above including, for example, from another aggregation point (e.g., the feed to the charging gateway, AAA server and/or mobile wireless center/HLR), one or

more of the gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720 the base station 125 and/or another network element. In some embodiments, the IPDR feeds from these or other network functions are copied to a database as described above, which is either pushed or queried to get the information to the service controller 122 or other network elements that request the IPDR information.

[0100] In some embodiments, the service processor 115 includes various components, such as device agents, that perform service policy implementation or management functions. In some embodiments, these functions include service policy or implementation verification, service policy implementation tamper prevention, service allowance or denial, application access control, traffic control, network access control services, various network authentication services, service control plane communication, device heartbeat services, service billing, transaction billing, simplified activation services and/or other service implementations or service policy implementations. It will be apparent to those of ordinary skill in the art that the division in functionality between one device agent and another is a design choice, that the functional lines can be re-drawn in any technically feasible way that the product designers see fit, and that the placing divisions on the naming and functional breakouts for device agents aids in understanding, although in more complex embodiments, for example, it can make sense to the product designer to break out device agent functionality specifications in some other manner in order to manage development specification and testing complexity and workflow.

[0101] In some embodiments, network control of the service policy settings and services as discussed above is accomplished with the service controller 122 which in various embodiments includes one or more server functions. As with the service processor 115 agent naming and functional break out, it is understood that service controller 122 server naming and functional breakout is also a design choice and is provided mainly to aid in the discussion. It will be apparent to those of ordinary skill in the art that the server names and functional breakouts do not imply that each name is an individual server, and, for example, a single named function in the various embodiments can be implemented on multiple servers, or multiple named functions in the various embodiments can be implemented on a single server.

[0102] As shown, there are multiple open content transaction partner sites 134 (e.g., open content transaction servers), which represent the websites or experience portals offered by content partners or ecommerce transaction partners of the service provider. For example, transaction servers 134 can provide an electronic commerce offering and transaction platform to the device. In some embodiments, the central provider has ownership and management of the service controller 122, so the central provider and the service provider are the same, but as discussed below the service provider that uses the service controller 122 to manage the device services by way of service processor 115 is not always the same as the central provider who provides the access network services.

[0103] In some embodiments, further distribution of central provider access networking functions such as access network AAA server 121, DNS/DHCP server 126, and other functions are provided in the base stations 125. In some embodiments, network based device service suspend/resume control are also provided in the base stations 125 (or in some embodiments, for hierarchical or overlay networks, this function is provided by one or more of the following: RAN gateways, transport gateways, AAA 121 or some other network function). As shown, the following are connected (e.g., in network communication with) the central provider network 110: central provider billing system 123, dedicated leased lines 128 (e.g., for other services/providers), central provider service controller 122, a content management (e.g., content switching, content billing, and content catching) system 130, central provider DNS/DHCP server 126, access network AAA server 121, service usage data store 118 and central provider mobile wireless center 132. These embodiments may be advantageous particularly for flat networks as that shown in FIG. 1 that are provided by the present invention.

[0104] In some embodiments, the base stations 125 implement a firewall function via firewall 124 and are placed directly onto the local loop Internet for backhaul. Voice traffic transport is provided with a secure protocol with Voice Over IP (VOIP) framing running over a secure IP session, for example, Virtual Private Network (VPN), IP Security (IPSEC) or another secure tunneling protocol. In some embodiments, the VOIP channel employs another layer of application level security on the aggregated VOIP traffic trunk before it is placed on the secure IP transport layer. Base station control traffic and other central provider traffic can be provided in a number of ways with secure transport protocols running over Transmission Control Protocol

(TCP), Internet Protocol (IP) or User Datagram Protocol (UDP), although TCP provides a more reliable delivery channel for control traffic that is not as sensitive to delay or jitter. One example embodiment for the control channel is a control link buffering, framing, encryption and secure transport protocol similar to that described below for the service control link between a device and the network. In some embodiments, a service control heartbeat function is provided to the base stations 125 similar to that implemented between the service controller 122 and the service processor 115 as described below. If the need to maintain a bandwidth efficient control plane channel between the base stations and the central provider base station control network is not as critical as it is in the case of access network connection to the device, then there are many other approaches for implementing a secure control channel over the Internet including, for example, one or more of various packet encryption protocols running at or just below the application layer, running TCP Transport Layer Security (TLS), and running IP level security or secure tunnels.

[0105] In some embodiments, the device based services control plane traffic channel between the service processor 115 and the service controller 122 is implemented over the same control plane channel used for the flat base station control architecture, or in some embodiments, over the Internet. As discussed below, it is assumed that the device bases services control plane channel for service processor 115 to service controller 122 communications is established through the Internet 120 or through the access network using IP protocols as this is the more general case and applies to overlay network applications for various embodiments as well as applications where various embodiments are used to enable flattened access networks.

[0106] In some embodiments, by enabling the device to verifiably implement a rich set of service features as described herein, and by enabling the base station 125 to connect directly to the Internet 120 with a local firewall for device data traffic, tunnel the voice to a voice network with VOIP and secure Internet protocols, and control the base station 125 over a secure control plane channel using base station control servers located in a central provider network, base stations 125 can be more efficiently provisioned and installed, because, for example, the base station 125 can accommodate a greater variety of local loop backhaul options. In such embodiments, it is advantageous to perform certain basic network functions in the base station 125 rather than the central provider network.

[0107] In some embodiments, a basic device suspend/resume function for allowing or disallowing the device Internet access is provided by the base stations 125 (or in some embodiments, for hierarchical or overlay networks in some embodiments this function is provided by one or more of the following: RAN gateways, transport gateways, AAA 121 or some other network function). This functionality, as will be discussed below, is important for certain embodiments involving taking action to resolve, for example, service policy verification errors. In some embodiments, this function is performed at the base station (e.g., base stations 125) thereby eliminating the need for a more complex networking equipment hierarchy and traffic concentration required to perform the suspend/resume function deeper in the network. Access network base stations control media access and are therefore designed with awareness of which device identification number a given traffic packet, group of packets, packet flow, voice connection or other traffic flow originates from and terminates to. In some embodiments, the suspend/resume function is implemented in the base station 125 by placing an access control function in the traffic path of each device traffic flow. The suspend resume function can be used by various network elements, and in the context of the present embodiment can be used by the service controller 122 (e.g., in some embodiments, access control integrity server 1654 (FIG. 16) of service controller 122 or other service controller elements) to suspend and resume device service based on the assessment of the service policy implementation verification status as described below.

[0108] In some embodiments, at least a basic traffic monitoring or service monitoring function is performed at the base station (e.g., base stations 125) similar to the service history records or IPDRs collected deeper in the network in more conventional hierarchical access network infrastructure architectures. For example, the service or traffic monitoring history records are advantageous for tracking device network service usage or service activity behavior and for certain verification methods for device based service policy implementation or higher device based services as discussed below. In some embodiments, a traffic monitoring function is provided in the base station 125 in which the traffic for each device is at least counted for total traffic usage and recorded. In some embodiments, traffic inspection beyond simply counting total traffic usage is provided. For example, the base station traffic monitor can record and report IP addresses or include a DNS lookup function to report IP addresses or IP addresses and associated Uniform Resource Locators (URLs). Another example allows the base station 125 to

attach location data to the IPDR to provide device location data in the records. In some embodiments, traffic inspection includes recording deeper levels of traffic or service monitoring.

[0109] In some embodiments, device traffic associated with service verification conditions indicating service usage is out of policy or profile limits or allowances is routed to a quarantine network rather than or as an initial alternative to a suspending service. For example, the advantages for this approach and a more detailed description of the quarantine network are discussed below. In some embodiments, the quarantine network capability is provided for in which rather than simply suspending device traffic completely from the network as described above, the base station 125 includes a firewall function (e.g., firewall 124) that is capable of passing device access traffic with the quarantine network destinations and blocking device access to all other destinations. In some embodiments, when it is discovered that service verification conditions indicate that service usage is out of policy or profile limits or allowances, then one or more of the following actions are taken: the user is notified of the overage condition, the user is required to acknowledge the overage condition, the user account is billed for the overage condition, and the device is flagged for further analysis by a network device analysis function or a network manager.

[0110] In some embodiments, network complexity is reduced using the device without moving completely to a flat base station network as described above. Device participation in the core network services implementation provides for numerous measures for simplifying or improving network architecture, functionality or performance. For example, two approaches are discussed below ranging from a simple overlay of the service processor 115 onto devices and the service controller 122 in a conventional hierarchical access network as illustrated in FIGS. 4 through 7, to a completely flat network as illustrated in FIGS. 1 through 3 and 8. Those of ordinary skill in the art will appreciate that the disclosed embodiments provided herein can be combined with the above embodiments and other embodiments involving flat network base stations to provide several advantages including, for example, richer service capability, less access network complexity, lower access network expenses, more flexible base station deployments, or less complex or less expensive base station back haul provisioning and service costs.

[0111] In most of the discussion that follows, the network based service history records and the network based suspend-resume functionality used in certain embodiments involving service implementation verification are assumed to be derived from the device service history 1618 (as shown in FIG. 16) central provider network element and the AAA server 121 central provider network element, and in some embodiments, working in conjunction with other central provider network elements. It is understood that these functions provided by the network can be rearranged to be provided by other networking equipment, including the base station as discussed above. It is also understood that the network based device traffic monitoring, recording and reporting to the device service history 1618 element can be accomplished at the base stations. Furthermore, it is understood that while the AAA server 121 is assumed to provide the suspend/resume functionality, quarantine network routing or limited network access called for in some embodiments, the AAA server 121 can be a management device in which the actual implementation of the traffic suspend/resume, firewall, routing, re-direction forwarding or traffic limiting mechanisms discussed in certain embodiments can be implemented in the base stations as discussed above or in another network element.

[0112] In some embodiments, an activation server 160 (or other activation sequencing apparatus) provides for provisioning, as described below, of the devices 100 and/or network elements in the central provider network so that, for example, the device credentials can be recognized for activation and/or service by the network. In some embodiments, the activation server 160 provides activation functions, as described below, so that, for example, the devices can be recognized by the network, gain access to the network, be provided with a service profile, be associated with a service account and/or be associated with a service plan. As shown in FIG. 1, the activation server 160 is connected to the central provider core network 110. In this configuration, the activation server 160 acts as, an over the network or over the air, activation function. In some embodiments, the activation server 160, or variations of the activation server 160 as described below, is connected to apparatus in the manufacturing or distribution channel, or over the Internet 120, or as part of the service controller 122 to service provisioning or activation functions. In some embodiments, the activation server 160 is connected to the central provider core network 110. In some embodiments, the activation server 160 is connected to other network extensions such as an MVNO network or the Internet 120 if, for example, the routers in the service gateways or base stations have the capability to direct traffic from devices

that are not fully activated or provisioned to an Internet destination, or if the service processor 115 is used for such direction. In some embodiments, the activation server 160 is included in the service controller 122.

[0113] FIG. 2 illustrates another simplified (e.g., “flattened”) network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments. As shown, an open MVNO configuration is provided in a simplified network as similarly described above with respect to FIG. 1. In some embodiments, the service provider (e.g., service owner) is defined by the entity that maintains and/or manages the service controller 122 associated with and controlling the service processors 115 that are inside the devices 100 using the service. In some embodiments, the service controller 122 requires only a non-real time relatively low data rate secure control plane communication link to the service processors 115. Accordingly, in some embodiments, the service controller 122 servers can reside in any network that can connect to (e.g., be in network communication with) the Internet 120. For example, this approach provides for a more efficient provisioning of the equipment used to set up an MVNO partnership between the central provider and the service provider, and as shown in FIG. 2, an MVNO network 210 is in network communication with the Internet 120 just as with the central provider network 110 is in network communication with the Internet 120. As shown, the following are connected to (e.g., in network communication with) the MVNO core network 210: MVNO billing system 123, MVNO service controller 122, MVNO content management system 130, MVNO DNS/DHCP server 126, MVNO AAA server 121, and MVNO mobile wireless center 132.

[0114] By showing two service controllers 122, one connected to (e.g., in network communication with) the MVNO network 210 and one connected to the central provider network 110, FIG. 2 also illustrates that some embodiments allow two entities on the same access network to each use the service controller 122 and service processor 115 to control different devices and offer different or similar services. As described below, the unique secure communication link pairing that exists between the two ends of the service control link, 1691 and 1638 (as shown in FIG. 16), ensure that the two service controllers 122 can only control the devices associated with the correct service provider service profiles.

[0115] FIG. 3 illustrates another simplified (e.g., “flattened”) network architecture including two central providers in accordance with some embodiments. For example, this provides for roaming agreements while maintaining rich services across different networks with completely different access layers. As shown, the mobile devices 100 are assumed to have a dual mode wireless modem that will operate on both a 4G network, for example LTE or WiMax, and a 3G network, for example HSPA or EVDO. One example roaming condition would be both Central Provider #1 and Central Provider #2 providing 3G and 4G network resources. In this example, the mobile devices 100 can connect to both 3G and 4G base stations 125 owned and operated by the central provider with whom they have signed up for service, or when neither is available from the central provider the user signed up with the device can roam onto the other central provider access network and still potentially offer the same rich service set using the same service profiles provided, for example, the roaming service costs are reasonable. In some embodiments, if roaming service costs are significantly more expensive than home network service costs, then the service processor 115 is configured with a roaming service profile that reduces or tailors service usage or service activity through a combination of one or more of user notification, user preference feedback regarding traffic shaping or service policy management preference collected and acted on by service processor 115, adaptive policy control in service processor 115 that tracks increasing roaming service costs and scales back service, or recognition of the change in network that causes the service controller 122 to configure service processor 115 of device 100 with a roaming service profile. In some embodiments, in roaming situations, network selection can be based on an automatic network selection with network selection being determined, for example, by a combination of user service profile preferences, service provider roaming deals and/or available roaming network capabilities and cost, as discussed further below.

[0116] In some embodiments, the devices 100 are again assumed to be multimode 3G and 4G devices (e.g., the mobile devices 100 are assumed to have a dual mode wireless modem that will operate on both a 4G network, for example LTE, and a 3G network, for example HSPA or EVDO), with the devices 100 being billed for service by Central Provider #1 being, for example, EVDO and LTE capable, and the devices 100 being billed for service by Central Provider #2 being, for example, HSPA and LTE capable. For example, the devices 100 can roam using the 4G LTE network of the roaming central provider when neither the 3G nor 4G

networks are available with the home central provider. As similarly discussed above with respect to the above described roaming embodiments, the service processors 115 and service controllers 122 are capable of providing similar services on the 4G roaming network and the 3G home network as on the 4G home network, however, the varying costs and available network capacity and speed differences of 3G home, 4G roaming and 4G home may also encourage the use of different, such as three different, service profiles to allow for the most effective and efficient selection and control of services based on the current network.

[0117] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments. As shown, FIG. 4 includes a 4G/3G/2G HSPA/Transport access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. In some embodiments, the central provider can offer improved service capabilities using a conventional UMTS network. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the conventional UMTS network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled across the various UMTS network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121. Referring now to the 4G/3G/2G HSPA/Transport access network as shown in FIG. 4, the LTE/HSPA and HSPA/GPRS base stations/nodes 125 are in communication with 4G/3G/2G Service/Serving GPRS Support Nodes (SGSNs) cluster 410 via a radio access network 405, which are in communication with 4G/3G/2G Gateway GPRS Support Nodes (GGSNs) cluster 420 via an access transport network 415 (e.g., a GPRS-IP network), which are then in communication with central provider core network 110.

[0118] As shown in FIG. 4, as discussed elsewhere, service usage data store 118 is a functional descriptor for a network level service usage information collection and reporting function located in one or more of the networking equipment boxes attached to one or more of the sub-networks in the figure (e.g., RAN, transport and/or core networks). As shown in FIG. 4, service usage 118 is shown as an isolated function connected to the central provider core network 110 and the intention of this depiction is to facilitate all the possible embodiments for

locating the service usage 118 function. In some UMTS network embodiments, the service usage 118 function is located or partially located in the GGSN gateway (or gateway cluster) 420. In some embodiments, service usage 118 functionality is located or partially located in the SGSN gateway (or gateway cluster) 410. In some embodiments, service usage 118 functionality is located or partially located in the equipment cluster that includes the AAA 121 and/or the mobile wireless center 132. In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station 125 in FIG. 4 and many other figures described herein. In some embodiments, service usage 118 functionality is located or partially located in a networking component in the transport network 415, a networking component in the core network 110, the billing system 123 and/or in another network component or function. This discussion on the possible locations for the network based service usage history logging and reporting function can be easily generalized to all the other figures described herein by one of ordinary skill in the art (e.g., RAN Gateway 410 and/or Transport Gateway 420), and this background will be assumed even if not directly stated in all discussion above and below.

[0119] In some embodiments, a central provider provides open development services to MVNO, Master Value Added Reseller (MVAR) and/or Original Equipment Manufacturer (OEM) partners. In some embodiments, all three service providers, central provider service provider, MVNO #1 service provider and MVNO #2 service provider have service control and billing control of their own respective devices 100 through the unique pairing of the service processors 115 and service controllers 122. For example, MVNO #1 and MVNO #2 can each have open development billing agreements with the central provider and each can own their respective billing systems 123. As shown in FIG. 4, MVNO #1 core network 210 is in communication with the central provider core network 110 via the Internet 120, and MVNO #2 core network 210 is in communication with the central provider core network 110 via an alternate landline(LL)/VPN connection 425. In some embodiments, the two MVNOs each offer completely different devices and/or services, and the devices and/or services also differ significantly from those offered by the central provider, and the service profiles are adapted as required to service the different devices and respective service offerings. In addition, the central billing system 123 allows all three service provider user populations to access ecommerce experiences from transaction provider partners operating transaction servers 134, to choose

central provider billing options that combine their third party transaction bills on their service provider bill, and each subscriber population can experience a service provider specified look and feel that is unique to the respective service provider even though the different user populations are interfacing to the same transaction servers and the transaction partners do not need to require significant custom development to provide the unique central billing and unique consistent user experience look and feel.

[0120] In some embodiments, a central provider offers open network device and service developer services using one service controller server 122 (e.g., a service controller server farm) and allows the open development partners to lease server time and server tools to build their own service profiles. The central provider also provides service billing on behalf of services to the open development partners. For example, this reduces costs associated with setting up an MVNO network for the open development partners and does not require the partners to give up significant control or flexibility in device and/or service control.

[0121] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments. This figure is similar to FIG. 4 except for the various particular variations of the EVDO network architecture as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill in the art. As shown, FIG. 5 includes an EVDO access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. The EVDO access network includes LTE/EVDO and EVDO/1xRTT base stations 125 in communication with Base Station Controller (BSC) packet control 508 and radio network controller 512 via a radio access network (RAN) 505, which are in communication with packet data service node 520 via an access transport network 515, which is in communication with central provider core network 110. As shown, a RAN AAA server 521 is also in communication with the access transport network 515.

[0122] In some embodiments, the central provider can offer improved service capabilities using a wireless access network. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure

control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

[0123] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments. This figure is also similar to FIG. 4 except for the various particular variations of the 4G LTE/Wi-Fi network architecture as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill. As shown, FIG. 6 includes a 4G LTE and Wi-Fi access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. The 4G LTE/Wi-Fi access network as shown includes LTE eNodeB and HSPA/EVDO base stations 125 in communication with Base Station Controller (BSC) packet control (EVDO & 1xRTT) 608 and SGSN (HSPA & GPRS) 612 via a radio access network (RAN) 605, which are in communication with System Architecture Evolution (SAE) Gateway (GW) 620 via an access transport network 615, which is then in communication with central provider (core) network 110. As shown, a Mobile Management Entity (MME) server 619 is also in communication with the access transport network 615. Also as shown, a Wi-Fi Access Point (AP) 602 is also in communication with the access transport network 615 via Wi-Fi Access Customer Premises Equipment (CPE) 604. As will be apparent to those of ordinary skill in the art, the embodiments of network architectures shown, for example, in FIGS. 1-8 are exemplary network architecture embodiments in which one or more of the shown network elements may not be required or included, alternative network elements included, and/or additional network elements included based on network design choices, network standards and/or other functional/design considerations and choices.

[0124] In some embodiments, the central provider can offer improved service capabilities using the wireless access network as depicted in FIG. 6. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

Accordingly, as shown in FIGS. 4 through 6, various embodiments can be implemented independent of the wireless access network technology, and for example, can be implemented in 3G, 4G and any other wireless access network technology.

[0125] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments. This figure is also similar to FIG. 4 except for the various particular variations of a combined WiMax/Wi-Fi network as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill in the art. As shown, FIG. 7 includes both a WiMax and Wi-Fi network (e.g., a combined WiMax/Wi-Fi network) operated by a central provider and two MVNO networks 210 operated by two MVNO partners. Although the Wi-Fi and WiMax access technologies are different wireless access networking technologies, with WiMax providing a wide area networking technology and Wi-Fi providing a local area networking technology, which efficiently operates using the two wireless access networking capabilities. As similarly discussed above with respect to the switching between 3G and 4G networks, some embodiments employ the automatic network selection capability as described above to choose the best available network service profile, and, for example, the user can force the decision or the service controller can make the decision. For example, if free Wi-Fi services have adequate coverage, in most cases, the decision criteria programmed into the automatic network selection algorithm will select Wi-Fi as long as the Wi-Fi access points are associated with a known and trusted provider. In some embodiments, transaction billing from central provider billing system 123 or MVNO #1 or MVNO #2 billing systems 123 will work with the transaction servers when connected over Wi-Fi just as when connected over any other access technology (including wire line based connections). The WiMax/Wi-Fi access network as shown includes WiMax base stations 125, Wi-Fi access points/hotspots 702 and/or Wi-Fi mesh access networks 702 (in some embodiments, femto cells can be used in addition to and/or as an alternative to Wi-Fi), and Wi-Fi access customer-premises equipment (CPE) 704 in communication with WiMax service controller 708 and Wi-Fi service controller 712 via a radio access network 705, which are in communication with WiMax core gateway 720 via an access transport network 715, which is then in communication with central provider (core) network 110.

[0126] In some embodiments, the central provider can offer improved service capabilities using the wireless access network as depicted in FIG. 7. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

[0127] Referring to FIG. 7, the Wi-Fi connection can be replaced with a femto cell (and the Wi-Fi modem shown in FIGS. 15D and 15E can be replaced with a femto cell modem (base station side functionality)). In some embodiments, the service processor 115 is provided on the femto cell to control subscriber access in a verifiable manner as similarly described herein with respect to various embodiments (e.g., the Wi-Fi related embodiments). For example, the femto cell service provider (e.g., the entity that owns the spectrum the femto cell is using) can operate the femto cell as a local access mechanism for the home subscriber (or other who purchased or installed the femto cell), and then also use it to provide pay-for-service or additional free services, with controlled access and/or traffic control and/or service control and/or billing control performed locally or in combination with network equipment as described herein. In some embodiments, the WWAN devices being used at home or work with the femto cell include a portion of the service processor functionality. For example, this allows the service provider for femto cells to provide service and monetize service in a controlled way even though the femto cell is not connected to the service provider network the way conventional base stations are connected to the service provider network, but is connected through the Internet 120. For example, the secure heartbeat function can be extended to include data traffic so that it is encrypted and secured along with the control plane traffic. The decision of whether or not to admit a device onto the femto cell can be made through the service processor 115 connection to the service controller 122 and subsequent look up of the credentials for the device and the associated service plan and service profile that is then programmed into the service processor on the femto cell and/or the device itself. The femto cell can also offer a landing page to devices through the service processor so that devices that do not belong to the network can gain access to the network by signing up over the femto cell. For example, the intermediate device embodiments for Wi-Fi on one end and WWAN on the other can be accomplished by using the

Wi-Fi connection in the cell phone in AP mode so that it becomes the intermediate device. The service processor 115 on the cell phone can then act in the same manner as described for the intermediate device as described herein.

[0128] FIG. 8 illustrates another simplified (e.g., “flattened”) network architecture including multiple wireless access networks (e.g., 3G and 4G Wireless Wide Area Networks (WWANs)) and multiple wire line networks (e.g., Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks) in accordance with some embodiments. It is a common network architecture for multi-access central providers to have one or more wired access networks and one or more wireless access networks. As shown, FIG. 8 includes both 3G and 4G wireless access networks, including a 4G base station 125 and a 3G base station 125, and both DOCSIS and DSLAM wire line networks (e.g., a combined WWAN/wire line network), including DOCSIS Head End 125 and DSLAM 125, operated by a central provider via central provider (core) network 110 and an MVNO partner via MVNO network 210 via the Internet 120.

[0129] As shown, the service processor 115 can reside on a number of different types of devices 100 that work on 3G or 4G wireless, DSL or DOCSIS, and the service controller 122 is capable of controlling each of these types of devices with a consistent service experience, for example, using different service profiles, service capabilities and service profile cost options depending on which network the device is connected to and/or other criteria. For example, a download of a High Definition (HD) movie can be allowed when the service controller 122 is managing service profile policies for a service processor 115 residing on a DOCSIS device 100 (e.g., a computer or laptop connected to a cable modem), but not when the same service controller 122 is managing service profile policies for a service processor 115 residing on a 3G device 100 (e.g., a smart phone connected to a mobile 3G network).

[0130] As will now be apparent to one of ordinary skill in the art in view of the above description of FIGS. 1 through 8, the present invention can be provided across any access network and a set of service profiles can be defined in a variety of ways including, for example, to user preference feedback, access network performance, access network cost, access network central provider partnership status with the service provider central provider and roaming deals

and costs. For example, as discussed below, various embodiments allow for users to have superior service experiences based on the ability to control certain of their service settings, and service providers can also more efficiently deploy a greater variety of services/service plans to users.

[0131] In some embodiments, the service processor 115 and the service controller 122 provide an overlay for existing networks without significantly changing the billing system 123, gateways/routers or other network components/elements, and also provide verifiable service monitoring to control services and/or service usage/costs without involving, for example, a service provider or MVNO (e.g., for smart phone devices and/or laptops or netbooks (or any other network accessible device) with an unlimited data plan or any other service plan). For example, applications that are deployed by device owners or service subscribers (e.g., an IT manager) and do not involve a service provider include roaming services provided as an after-market product without carrier/service provider involvement. In this example, device activity is recorded by the service processor 115 and transmitted to the service controller 122 (e.g., the IT manager controls the service controller 122). In another example, a third party after-market product is provided in which the service controller 122 is hosted by the third party and the device management entity (e.g., the IT manager or parents of the device user for parental controls) uses a secure Virtual Service Provider (VSP) website to control the devices that belong to that management entity's device partition (e.g., VSP partitions and techniques are described below with respect to FIG. 49). The VSP secure website techniques described herein can also be applied to service provider owned servers with device partitions for the purpose of controlling, for example, Deep Packet Inspection (DPI) controllers (e.g., DPC policy implementation 5402 as shown in FIG. 54) to provide similar or substantially equivalent service usage/control capabilities using network based service control techniques, as similarly described in detail below with respect to FIGS. 49 and 54 (e.g., IT manager VSP control of a group partition and/or MVNO VSP control of a group partition).

Service Processor Configurations for Devices

[0132] FIG. 9 illustrates a hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 9, the service processor

115 is stored in a non volatile memory 910 and a memory 920 of the device 100. As will be appreciated by those of ordinary skill in the art, the present invention can operate with virtually any device architecture, and the device architectures discussed herein (e.g., with respect to FIGS. 9-14 and 15A-15F) are examples of various implementations on certain devices (e.g., of different representations of device 100).

[0133] As shown in FIG. 9, device 100 also includes a processor 930, sometimes referred to as a CPU or central processor unit, an APU or application processor unit, a core processor, a computing device, or many other well known terms. In some embodiments, device 100 includes one or more processors and/or a multicore processor. As shown, processor 930 includes a sub-processor 935. In some embodiments, processor 930 and/or sub-processor 935 are based on an architecture sometimes referred to as a complex instruction set computer or CISC, a reduced instruction set computer or RISC, a parallel processor, a combination of two or more architectures or any other processor architecture. In some embodiments, processor 930 has a design that is based on logic and circuitry from one or more standard design library or published architecture, or includes specialized logic and circuitry designed for a given device 100 or collection of such devices. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, one processor and/or sub-processor can have one architecture while another may have a somewhat different or completely different architecture. In some embodiments, one or more of the processors and/or sub-processors can have a general purpose architecture or instruction set, can have an architecture or instruction set that is partially general or partially specialized, or can have an instruction set or architecture that is entirely specialized. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, there can be a division of the functionality for one or more processors and/or sub-processors. For example, one or more processors and/or sub-processors can perform general operating system or application program execution functions, while one or more others can perform communication modem functions, input/output functions, user interface functions, graphics or multimedia functions, communication stack functions, security functions, memory management or direct memory access functions, computing functions, and/or can share in these or other specialized or partially specialized functions. In some embodiments, any processor 930 and/or any sub-processor 935 can run a low level operating system, a high level operating system, a combination of low level and high level operating systems, or can include

logic implemented in hardware and/or software that does not depend on the divisions of functionality or hierarchy of processing functionality common to operating systems.

[0134] As shown in FIG. 9, device 100 also includes non-volatile memory 910, memory 920, graphics memory 950 and/or other memory used for general and/or specialized purposes. As shown, device 100 also includes a graphics processor 938 (e.g., for graphics processing functions). In some embodiments, graphics processing functions are performed by processor 930 and/or sub-processor 935, and a separate graphics process 938 is not included in device 100. As shown in FIG. 9, device 100 includes the following modems: wire line modem 940, WWAN modem 942, USB modem 944, Wi-Fi modem 946, Bluetooth modem 948, and Ethernet modem 949. In some embodiments, device 100 includes one or more of these modems and/or other modems (e.g., for other networking/access technologies). In some embodiments, some or all of the functions performed by one or more of these modems are performed by the processor 930 and/or sub processor 935. For example, processor 930 can implement some or all of certain WWAN functional aspects, such as the modem management, modem physical layer and/or MAC layer DSP, modem I/O, modem radio circuit interface, or other aspects of modem operation. In some embodiments, processor 930 as functionality discussed above is provided in a separate specialized processor as similarly shown with respect to the graphics and/or multimedia processor 938.

[0135] As also shown in FIG. 9, device 100 includes an internal (or external) communication bus structure 960. The internal communication bus structure 960 generally connects the components in the device 100 to one another (e.g., allows for intercommunication). In some embodiments, the internal communication bus structure 960 is based on one or more general purpose buses, such as AMBA, AHP, USB, PCIe, GPIO, UART, SPI, I²C, Fire wire, DisplayPort, Ethernet, Wi-Fi, Bluetooth, Zigbee, IRDA, and/or any other bus and/or I/O standards (open or proprietary). In some embodiments, the bus structure is constructed with one or more custom serial or parallel interconnect logic or protocol schemes. As will be apparent to one of ordinary skill in the art, any of these or other bus schemes can be used in isolation and/or in combination for various interconnections between device 100 components.

[0136] In some embodiments, all or a portion of the service processor 115 functions disclosed herein are implemented in software. In some embodiments, all or a portion of the service processor 115 functions are implemented in hardware. In some embodiments, all or substantially all of the service processor 115 functionality (as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device 100. FIG. 9 illustrates an embodiment in which service processor 115 is stored in device memory, as shown, in memory 920 and/or non-volatile memory 910, or a combination of both. In some embodiments, it is advantageous to store or implement certain portions or all of service processor 115 in protected or secure memory so that other undesired programs (and/or unauthorized users) have difficulty accessing the functions or software in service processor 115. In some embodiments, service processor 115, at least in part, is implemented in and/or stored on secure non-volatile memory (e.g., non volatile memory 930 can be secure non-volatile memory) that is not accessible without pass keys and/or other security mechanisms. In some embodiments, the ability to load at least a portion of service processor 115 software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor 115 software components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader 1663 as discussed below (and as shown in FIG. 16). In some embodiments, a secure software download embodiment also uses a secure non-volatile memory. Those of ordinary skill in the art will also appreciate that all memory can be on-chip, off-chip, on-board and/or off-board. In some embodiments, the service processor 115 which as shown in FIG. 9 is stored or implemented in non volatile memory 910 and memory 920, can be implemented in part on other components in device 100.

[0137] As shown, device 100 also includes a user interfaces device component 980 for communicating with user interface devices (e.g., keyboards, displays and/or other interface devices) and other I/O devices component 985 for communicating with other I/O devices. User interface devices, such as keyboards, display screens, touch screens, specialized buttons or switches, speakers, and/or other user interface devices provide various interfaces for allowing one or more users to use the device 100.

[0138] FIG. 10 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 10, the service processor 115 is implemented on the processor 930 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the processor 930. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the processor 930. While the service processor 115 is shown in FIG. 10 as stored, implemented and/or executed on the processor 930, in other embodiments, the service processor 115 is implemented in part on other components in device 100, for example, as discussed below.

Service Processor Implemented on a Communications Modem

[0139] FIG. 11 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 11, the service processor 115 is implemented on the WWAN modem 942 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the WWAN modem 942. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the WWAN modem 942. In some embodiments, service process 115 is implemented on another modem component of device 100 and/or one or more of the modem components of device 100.

[0140] In some embodiments, the service processor 115 is implemented on a modem processor (e.g., WWAN modem 942 or WWAN/Wi-Fi modem), and the service processor 115 can be installed and/or executed in protected and/or secure memory or processor hardware on the modem. The modem memory can be made robust to hacking or tampering and, in some embodiments, is only accessible from a secure network management channel or secure device management port and not by most end users. In some embodiments, a portion of the service processor 115 is implemented on a modem processor (e.g., WWAN modem 942 hardware or software), and a portion of the service processor 115 is implemented on another device 100 processor 930. For example, the device service monitor agent 1696 and one or more service usage measurement points (see discussion associated with FIG. 21) can be implemented on a modem processor, and other service processor 115 elements can be implemented in the main

device operating system processor 930. As another example, a second (or first) service monitor agent 1696 and one or more service usage measurement points can be implemented on a modem processor, and a first (or second) service monitor 1696 with one or more service measurement points can be implemented on the main operating system processor 930 for device 100. For example, such embodiments can be configured to provide a service usage measurement and reporting system that offers a diversified countermeasure to protect against hacking, tampering or other errors for device based service usage measurements that can be made harder to hack or tamper with than certain software embodiments on the processor 930. For example, such embodiments can be employed when one or more of the following capabilities are not available: network based service usage measures, network based service profile or policy implementation verification measures, and network based service usage verification error response action capabilities.

[0141] In some embodiments, certain portions of the service processor 115 that deal with application layer service monitoring or traffic flow identification (e.g., tagging or traffic flow shaping as disclosed elsewhere) are implemented on a main processor 930, and other portions of the service processor 115 are implemented on a modem processor (e.g., WWAN modem 942).

[0142] In some embodiments, the WWAN modem is a wide area access technology modem such as 2G, 2.5G, 3G or 4G. As discussed above and below, the connection to the WWAN modem 942 can be a connection internal to device 100, for example a USB, GPIO, AMBA or other bus, or can be a connection that extends external to the device such as for example a USB, Ethernet, Wi-Fi, Bluetooth or other LAN or PAN connection. Three example embodiments in which the bus is internal to the device are as follows: a PCIe modem card running over USB or PCIe, a GPIO connection running from a processor 930 chipset to a modem chipset inside a mobile device, or a Wi-Fi connection running from a Wi-Fi modem inside of device 100 to an intermediate modem or networking device combination that forwards the access network traffic between the access network connection and the device via the Wi-Fi connection. In some embodiments, in addition to the service processor 115 being implemented on the WWAN modem 942 either internal or external to the device 100, similarly service processor 115 can be implemented on a wire line modem 940, such as DSL, Cable or fiber, another wireless LAN or PAN modem, such as Wi-Fi, Zigbee, Bluetooth modem 948, White Space, or some other

modem, connected internal to device 100 or external to device 100 via a LAN or PAN extension of internal or external communications bus structure 960.

[0143] In some embodiments, a complete turn-key reference design product for the device modem (one or more of 942, 946, 948, 949, 944, 940) combined with a built-in service processor 115, possibly with a well defined and documented application interface and a well defined and documented service processor developers kit (SPDK) provides for a powerful product embodiment for the purpose of achieving mass market distribution and usage for the modem with service processor 115 and associated service controller 122 features. For example, embodiments that include the WWAN modem 942, possibly in combination with one or more additional modems including Wi-Fi modem 946, bluetooth modem 948, USB modem 944 and Ethernet modem 949, can be combined with a pre-tested or pre-certified integrated embodiment of the service processor 115, possibly in combination with a well defined API for writing software applications that interface to, reside on or communicate with this turn-key modem embodiment. As disclosed herein, the advantageous capabilities of the service processor 115, possibly in conjunction with the service controller 122, to assist in monitoring, control, billing and verification for services is made more available for device 100 manufacturers in such a form, because the manufacturers do not need to spend as much time and resources to develop a custom modem only for a subset of devices that the turn-key modem can be used to support. In some embodiments, the service processor 115, as discussed herein, can be configured to provide device assisted service monitoring, control, billing and/or verification across not just when connected to the WWAN network via the WWAN modem, but also when connected to the other networks corresponding to the other access modems included in the turn-key combined module plus service processor 115 (or SPDK or chipset plus service processor 115) design. The pre-integrated service processor 115 and API possibly in combination with testing and certification can be packaged in a small form factor that may have standardized interfaces such as USB, PCIe, firewire, Display Port, GPIO, or other interface. The form factor may be miniaturized into standard configurations such as minicard, half minicard or even smaller form factors, or it can be designed into a non-standard or proprietary form factor. The module form factor can be well documented to simplify integration into various device 100 designs. The SPDK embodiments can be designed to contain one or more of the following: hardware integration and use documentation, software integration documentation, software programming documentation,

application interface documentation, service controller documentation, overall testing guidelines and overall use guidelines. In some embodiments, the modem module can be integrated with the service processor 115 functionality as a combined chipset, firmware and/or software product, with other SPDK features very similar to those listed above. The service controller programming guide for these turn-key embodiments can also be documented for the SPDK service processor 115 software, turn-key module with service processor 115 or integrated chipset with service processor 115. Accordingly, these embodiments provide various solutions to simplify the OEM task of integrating, developing, testing and shipping device 100 products (or integrated networking device products) with any of the device assisted service monitoring, control, billing or verification capabilities disclosed herein.

[0144] FIG. 12 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 12, the service processor 115 is implemented on the other I/O devices component 980 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the other I/O devices component 980 (e.g., a SIM/USIM card or other secure hardware I/O device). In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the other I/O devices component 980.

[0145] As discussed above, various embodiments include product designs in which the service processor 115 resides on device volatile or non-volatile memory (see FIG. 9), the device application processor or CPU (see FIG. 10), the wireless access modem (see FIG. 11) (or any other modem), or another I/O device (see FIG. 12). While these are just a few of the example service processor 115 placement embodiments, these embodiments show that the placement of where the software or hardware for implementing the service processor 115 can reside in the device 100 is very flexible and can be implemented in a myriad of places and ways depending on the device and/or other technical design choices.

[0146] FIG. 13 illustrates another hardware diagram of a device 100 that includes a service processor 115 implemented in external memory of a System On Chip (SOC) 1310 in accordance with some embodiments. As shown in FIG. 13, the service processor 115 is

implemented on the external memory 1320 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the external memory 1320. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the external memory 1320. In some embodiments, SOC chipset 1310 and external memory 1320 provide a portion or all of the hardware of device 100.

[0147] FIG. 14 illustrates another hardware diagram of a device 100 that includes a service processor 115 implemented in external memory of a System On Chip (SOC) 1310 in accordance with some embodiments. As shown, the service processor 115 is stored in a non volatile memory 910 and a memory 920 of the SOC chipset 1310, as similarly discussed above with respect to FIG. 9. In some embodiments, SOC chipset 1310 and external memory 1320 provide a portion or all of the hardware of device 100.

[0148] As similarly discussed above with respect to FIGS. 9 through 12, various embodiments include product designs including the SOC chipset 1310 in which the service processor 115 resides on internal volatile or non-volatile memory 910 of the SOC chipset 1310 (see FIG. 14), the device application processor or CPU 930 and/or sub processor 935, the modems 940, 942, 944, 946, 948, and/or 949 (or any other modem), another I/O device 985, and/or external memory 1320 (see FIG. 13) (and/or any combinations thereof). While these are just a few of the example service processor 115 placement embodiments, these embodiments show that the placement of where the software or hardware for implementing the service processor 115 can reside in the SOC chipset 1310 and/or the external memory 1320 of the device 100 is very flexible and can be implemented in a myriad of places and ways depending on the device and/or other technical design choices.

[0149] The above discussion with respect to FIGS. 9 through 14 illustrating various internal hardware embodiments for device 100 applies equally to this partitioning of device functionality or any other partitioning of how the components in device 100 are configured, whether they are all separate components, some of the components are combined into a single chipset but there are still multiple chipsets, or all of the components are combined into a chipset. For example, FIGS. 9 through 14 illustrating various internal hardware embodiments for device

100 show several access modem components including the wire line modem 940, wireless wide area network (WWAN) modem 942, USB modem 944, Wi-Fi modem 946, Bluetooth modem 948, and Ethernet modem 949. In some embodiments, wire line modem 940 is a DSL or cable modem such as DOCSIS, or some other modem with a hard connection such as fiber. In some embodiments, as discussed above and below, connection to the wire line or wireless access network is accomplished through an extension of the internal or external communications bus structure 960. For example, such an extension is accomplished using one or the other modems, such as Wi-Fi modem 946 or Ethernet modem 949, connecting to a local area network that in turn connects to the access network via a device that bridges the local area network to the access network. One of ordinary skill in the art will appreciate that when discussing device connection to any access network the connection can be via a direct connection to the network, such as a 3G or 4G WWAN modem 942 connection to a 3G or 4G WWAN network, or can be a connection to the access network through an intermediate connection, such as a Wi-Fi modem 946 connection to a modem or networking device combination that has a Wi-Fi LAN connection and a 3G or 4G network access network connection. Another example of an extended modem connection embodiment includes a Wi-Fi modem 946 device connection to a modem or networking device combination that includes a Wi-Fi LAN connection and a DOCSIS or DSL network access connection. Other examples of such combinations will be readily apparent to one of ordinary skill in the art.

Service Processor Configurations for Intermediate Networking Devices

[0150] FIGS. 15A through 15F illustrate hardware diagrams of a device 100 that include a service processor 115 and a bus structure extension 1510 using intermediate modem or networking device combinations in accordance with various embodiments. For example, FIGS. 15A through 15E illustrate various extended modem alternatives for access network connection through an intermediate modem or networking device combination that has a connection (e.g., LAN connection) to one or more devices 100.

[0151] In some embodiments, device 100 includes a 3G and/or 4G network access connection in combination with the Wi-Fi LAN connection to the device 100. For example, the intermediate device or networking device combination can be a device that simply translates the

Wi-Fi data to the WWAN access network without implementing any portion of the service processor 115 as shown in FIG. 15B. In some embodiments, an intermediate device or networking device combination includes a more sophisticated implementation including a networking stack and some embodiments a processor, as is the case for example if the intermediate networking device or networking device combination includes a router function, in which case the service processor 115 can be implemented in part or entirely on the intermediate modem or networking device combination. The intermediate modem or networking device combination can also be a multi-user device in which more than one user is gaining access to the 3G or 4G access network via the Wi-Fi LAN connection. In the case of such a multi-user network, the access network connection can include several managed service links using multiple instantiations of service processor 115, each instantiation, for example, being implemented in whole or in part on device 100 with the intermediate modem or networking device combination only providing the translation services from the Wi-Fi LAN to the WWAN access network.

[0152] Referring now to FIGS. 15A, 15C, 15D, and 15E, in some embodiments, the service processors 115 are implemented in part or in whole on the intermediate modem or networking device combination. In the case where the service processor 115 is implemented in part or in whole on the intermediate modem or networking device combination, the service processor 115 can be implemented for each device or each user in the network so that there are multiple managed service provider accounts all gaining access through the same intermediate modem or networking device combination. In some embodiments, the functions of service processor 115 are implemented on an aggregate account that includes the WWAN access network traffic for all of the users or devices connected to the Wi-Fi LAN serviced by the intermediate modem or networking device combination. In some embodiments, the central provider can also provide an aggregated account service plan, such as a family plan, a corporate user group plan and/or an instant hotspot plan. In the case where there is one account for the intermediate modem or networking device combination, the intermediate modem or networking device combination can implement a local division of services to one or more devices 100 or users in which the services are controlled or managed by the intermediate modem or networking device combination or the device 100, but the management is not subject to service provider control and is auxiliary to the service management or service policy implementation performed

by service processors 115. In some embodiments, another service model can also be supported in which there is an aggregate service provider plan associated with one intermediate modem or networking device combination, or a group of intermediate modems or networking device combinations but where each user or device still has its own service plan that is a sub-plan under the aggregate plan so that each user or device has independent service policy implementation with a unique instantiation of service processor 115 rather than aggregate service policy implementation across multiple users in the group with a single instantiation of service processor 115.

[0153] As shown in FIGS. 15A and 15C, in some embodiments, device 100 includes a Wi-Fi modem 946, a Wi-Fi modem 946 combined with a 3G and/or 4G WWAN modem 1530 on intermediate modem or networking device combination 1510, and the intermediate modem or networking device combination forwards WWAN access network traffic to and from device 100 via the Wi-Fi link. For example, the service processor 115 can be implemented in its entirety on device 100 and the service provider account can be associated exclusively with one device. This is an embodiment associated with one or more of FIGS. 29, 31, 32 or 34 discussed below, in which the modem bus represents the Wi-Fi LAN connection via the Wi-Fi modem 946. Similarly, as shown in FIGS. 15A and 15D, such an implementation can be provided using a different access modem and access network, such as a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use DSL as shown in FIGS. 15A and 15E, USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0154] In some embodiments, a portion of the service processor 115 is implemented on the device 100, such as the application interface agent 1693 and other supporting agents (see FIG. 16), and another portion of the service provider 115 is implemented on the intermediate modem or networking device combination, such as policy implementation agent 1690 or possibly modem firewall 1655 as well as other agents (see FIG. 16). This is an embodiment associated with one or more of FIGS. 30 or 36 discussed below, in which the modem bus in the figure represents the Wi-Fi LAN connection via the Wi-Fi modem 946. In this example, the

service provider 115 can still offer individual service plans associated exclusively with one device, or can offer an aggregate plan in which the portion of the service processor 115 located on the intermediate modem or networking device combination 1510 aggregates service plans into one WWAN connection but each individual device 100 has a unique service interface via the application interface agents and associated agents located on device 100. Similarly, such an implementation can be provided using a different access modem and access network, for example a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0155] In some embodiments, all of the service processor 115 is implemented on the intermediate modem or networking device combination 1510 and the aggregate device or user traffic demand from the LAN port is serviced through one service provider service plan account. This is an embodiment associated with FIG. 35 in which as discussed below the modem bus in the figure represents the Wi-Fi LAN connection via the Wi-Fi modem 946. Similarly, such an implementation can be provided using a different access modem and access network, for example a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0156] In some embodiments, the device 100 uses the on-board WWAN modem 942 when it is outside of Wi-Fi LAN coverage area for one or more trusted access networks for the device, and when the device comes within range of a Wi-Fi network associated with a intermediate modem or networking device combination connected to a trusted wire line access network, the device can switch to the Wi-Fi link service to connect service processor 115 to the trusted wire line access network. In some embodiments, the decision to switch to the Wi-Fi LAN associated with a trusted wire line access network can be made automatically by the device based on the policy implementation rules settings for the modem selection and control 1811

and/or the policy control agent 1692, can be made by the user, or can be made by the service controller 122 (see FIG. 18). In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0157] FIG. 15F illustrates another hardware diagram of a device 100 that includes a service processor 115 and a bus structure extension 1510 using intermediate modem or networking device combinations in accordance with various embodiments. In some embodiments, more than one access network connection is implemented in the intermediate modem or networking device combination 1510. This allows the device 100 to potentially connect through the intermediate modem or networking device combination with a choice of access network services. An example of such an embodiment is illustrated in FIG. 15F in which an access network router (e.g., an enterprise router) connected to a LAN with a wire line primary backhaul connection and a back up WWAN connection, for example 3G or 4G, to provide access services when the primary wire line connection fails. As discussed above, the service provider service profile for service processor 115 and the service plan account can be set up as an aggregate account with multiple users connected to the LAN. The service provider can elect to use an embodiment that includes a portion of the service processor 115 on each device 100 so that the account can be managed for each user or each device, or the service provider can elect to implement all of the necessary features in the service processor 115 on the intermediate modem or networking device combination so that there is no visibility to the individual devices 100 or users.

[0158] As described herein, various embodiments provide many service policy implementation options that can enhance the service provider control of the service experience and cost, or enhance the user control of the service experience and cost by providing a verifiable or compromise resistant solutions to manage service policy implementation on the intermediate modem or networking device combination, for one or both of the WWAN or wire line access networks, when the WWAN access network is active, or when the WWAN access network is inactive. The level of service control, user preference feedback and service policy implementation verification or compromise resistance enabled by these embodiments improves the offered back up services and primary wire line services. One of ordinary skill in the art will

also now appreciate that any number of wire line and/or wireless network access connections can be supported by the various embodiments as described herein, with any number of device architectures and architectures for intermediate modem or networking device combinations bridging the device to the access network of choice. Accordingly, various embodiments provide a verifiable managed service architecture, design and implementation for any number of single access and/or multi-access networks in which the service account can be consistent across multiple networks, and the service policies can be changed from network to network as deemed appropriate by the service provider with service notification, service cost control and privacy preference inputs from the user.

[0159] In various embodiments, the verification embodiments discussed herein for service policy implementation verification or service policy implementation compromise protection can be applied. In some embodiments, rather than attaching a service provider service plan account to a single device, it is attached to (e.g., associated with) a user. For example, when the user logs onto an access network with a service controller controlled by a service provider, regardless of what device the user logs onto with the user's service plan profile can be automatically looked up in the central billing system 123 and dynamically loaded (e.g., downloaded) onto the device 100 from the service controller 122 (e.g., a service profile provided on demand based on the user's identity). In some embodiments, in addition to dynamically loading the user's service policy implementation and control settings, one or more of the user's preferences including notification, service control, traffic monitor reporting privacy and Customer Relationship Management (CRM) reporting privacy are also dynamically loaded. For example, this allows the user to have the same service settings, performance and experience regardless of the device the user is logged into and using on the network. In addition, as discussed herein, in the various embodiments that call for roaming from one type of access network to another, the user service plan profile, that includes all of the above in addition to the service plan profile changes that take effect between different types of access network, can be used on any device and on any network, providing the user with a verifiable or compromise resistant, consistent service experience regardless of network or device.

[0160] Many of the embodiments described herein refer to a user using device 100. It is understood that there are also applications for these various embodiments that do not involve

user interfaces. Examples of such applications include equipment, apparatus or devices for automation, telemetry, sensors, security or surveillance, appliance control, remote machine to machine data connections, certain remote access configurations, two way power metering or control, asset tracking, people tracking or other applications in which a human user interface is not required for device 100.

[0161] Various embodiments of the device 100 described above include other I/O devices 985. In some embodiments, these other devices include other modems, other special purpose hardware components, and/or other I/O devices or drivers or modems to connect to other I/O devices. In some embodiments, these other devices include a Subscriber Identity Module (SIM) or Universal Subscriber Identity Module (USIM) device. In some embodiments, it is advantageous to implement some or all of the service processor 115 functions on an embodiment of device 100 that includes a SIM and/or a USIM. In some embodiments, the other I/O devices 985 include a hardware device designed to implement a portion or all of the service processor 115 functions. For example, this is advantageous in cases in which the original device 100 was not manufactured with the service processor 115; in cases in which dedicated hardware is desired to improve one or more aspects of service processor 115 performance; allowing users, for example, to have the same service settings, performance and experience regardless of the device the user is using on the network by using such a SIM and/or USIM (e.g., or implemented as a type of dongle); and/or in cases in which a separate component is desired to assist in compromise protection for one or more aspects of service processor 115.

[0162] As discussed above, some embodiments described herein provide for billing of certain access services. In some embodiments, various applications do not require or involve billing of certain services. For example, applications like enterprise IT (Information Technology) group management of enterprise workforce access policy implementation or access cost control or access security policy, privacy control, parental control, network quality of service control or enhancement, private network services, free access services, publicly funded access services, flat rate no-options service and other services, or other examples that will be apparent to one of ordinary skill in the art do not require billing functionality but benefit from many other aspects of various embodiments.

[0163] Service Processor and Service Controller for Verifiable Service Monitoring, Notification and Control

[0164] FIG. 16 is a functional diagram illustrating a device based service processor 115 and a service controller 122 in accordance with some embodiments. For example, this provides relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller 122 is connected to the Internet 120 and not directly to the access network 1610. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As previously discussed, it is understood that the division in functionality between one device agent and another is based on, for example, design choices, networking environments, devices and/or services/applications, and various different combinations can be used in various different implementations. For example, the functional lines can be re-drawn in any way that the product designers see fit. As shown, this includes certain divisions and functional breakouts for device agents as an illustrative implementation, although other, potentially more complex, embodiments can include different divisions and functional breakouts for device agent functionality specifications, for example, in order to manage development specification and testing complexity and workflow. In addition, the placement of the agents that operate, interact with or monitor the data path can be moved or re-ordered in various embodiments. For example, as discussed below in some embodiments, one or more of the policy implementation or service monitoring functions can be placed on one of the access modems located below the modem driver and modem bus in the communication stack as illustrated in certain figures and described herein. As discussed below, some simplified embodiment figures illustrate that not all the functions illustrated in all the figures are necessary for many designs, so a product/service designer can choose to implement those functions believed to be most advantageous or sufficient for the desired purposes and/or environment. The functional elements shown in FIG. 16 are described below.

[0165] As shown, service processor 115 includes a service control device link 1691. For example, as device based service control techniques involving supervision across a network become more sophisticated, it becomes increasingly important to have an efficient and flexible

control plane communication link between the device agents and the network elements communicating with, controlling, monitoring, or verifying service policy. In some embodiments, the service control device link 1691 provides the device side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions. In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security or encryption are used to make the link robust to discovery, eavesdropping or compromise. In some embodiments, the service control device link 1691 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments disclosed herein for the service control device link 1691 provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements.

[0166] In some embodiments, the service control device link 1691 agent messages are transmitted asynchronously as they are generated by one or more of the service agents. In some embodiments, the service control device link 1691 performs collection or buffering of agent messages between transmissions. In some embodiments, the service control device link 1691 determines when to transmit based potentially on several parameters including, for example, one or more of the following parameters: periodic timer trigger, waiting until a certain amount of service usage or traffic usage has occurred, responding to a service controller message, responding to a service controller request, initiated by one or more agents, initiated by a verification error condition, initiated by some other error or status condition. In some embodiments, once a transmission trigger has occurred, the service control device link 1691 assembles all buffered agent communications and frames the communications.

[0167] In some embodiments, the transmission trigger is controlled by waiting for an amount of service usage, such as waiting until a certain amount of data traffic has passed, which reduces the control plane communication channel traffic usage to a fraction of the data plane traffic. For example, this approach preserves network capacity and reduces service cost even in traffic scenarios in which data traffic is light.

[0168] In some embodiments, the transmission trigger is based on waiting for an amount of service usage, and also including a minimum transmission rate that triggers a transmission according to one or more of the following parameters: a maximum time between transmissions clock to keep the service processor 115 in communication with the service controller 122 when little or no service usage is occurring, a polling request of some kind from the service controller 122, a response to a service controller heartbeat, a transmission generated by a service verification error event, or a transmission generated by some other asynchronous event with time critical service processor 115 (or service controller 122) messaging needs, such as a transaction or service billing event or a user request. For example, service control plane traffic down is reduced to a relatively inexpensive and capacity conserving trickle when device 100 data traffic is not significant. At the same time, this approach also provides an effective flow of real time or near real-time service control plane traffic that is both cost and capacity efficient, because the service control plane traffic is a relatively small percentage of the data plane traffic when data plane traffic usage is heavy. For example, when data plane traffic usage is heavy is generally the time when close monitoring of service policy implementation verification or compromise prevention can be particularly important and by keeping the control plane overhead to a fraction of data plane traffic close monitoring and control of services are maintained at a reasonable cost in terms of percentage of both bandwidth used and network capacity. In some embodiments, the service usage or service activity trigger occurs based on some other measure than traffic usage, such as a number of messages transacted, one or more billing events, number of files downloaded, number of applications run or time that an application has been running, usage of one or more specified applications, GPS coordinate changes, roaming event, an event related to another network connection to the device and/or other service related measures.

[0169] In some embodiments, the service control device link 1691 provides for securing, signing, encrypting or otherwise protecting communications before sending. For example, the service control device link 1691 can send to the transport layer or directly to the link layer for transmission. In some embodiments, the communications are further secured with transport layer encryption, such as TCP TLS (Transport Control Protocol Transport Layer Security) or another secure transport layer protocol. In some embodiments, communications are encrypted at the link layer, such as IPSEC (Internet Protocol Security), various VPN (Virtual Private

Network) services, other forms of IP layer encryption and/or another link layer encryption technique.

[0170] In some embodiments, the service control link 1691 includes the above discussed agent heartbeat function in which the agents provide certain required reports to the service controller 122 for the purpose of service policy implementation verification (e.g., verification related reports on certain aspects of the service processor 115) or for other purposes. For example, such agent heartbeat messages can be in the open/clear (unencrypted) or encrypted, signed and/or otherwise secured. In some embodiments, these messages include one or more of the below described types of messages: an agent information message, an agent check-in message and/or agent cross check message.

[0171] In some embodiments, an agent information message is included in the agent heartbeat service policy implementation verification message, which includes, for example, any information the agent needs to communicate to the service controller 122 as part of the operation of the service policy implementation system. For example, an agent response to a service controller challenge, as described below, can be included in the agent heartbeat service policy implementation verification message.

[0172] In some embodiments, an agent check-in message is included in an agent heartbeat service policy implementation verification message, which includes, for example, a transmission of a unique agent identifier, secure unique identifier, and/or hashed encrypted and signed message beginning with some shared secret or state variable for the hash. For example, an agent self-check can be included in the agent heartbeat service policy implementation verification message, which includes reporting on agent configuration, agent operation, agent code status, agent communication log, agent error flags, and/or other agent associated information potentially hashed, encrypted, signed or otherwise secured in the message (e.g., using a shared secret unique to that agent).

[0173] In some embodiments, an agent cross-check message is included in the agent heartbeat service policy implementation verification message, which includes, for example, reports on the status, configuration, operation observations, communication log or other aspects of another agent. For example, agent environment reports can be included in the agent heartbeat

service policy implementation verification message, which includes, for example, reports on certain aspects of the service processor 115 operating environment, such as software presence (e.g., installation status of certain operating system and/or application software and/or components thereof), observed communication with agents or communication attempts, memory accesses or access attempts, network accesses or access attempts, software downloads or attempted downloads, software removal or download blocking, service policy implementation verification or compromise event error conditions with respect to the operating environment for the service processor 115, and/or other messages regarding the verification or possibility of compromise associated with the service processor 115 operating environment or agents.

[0174] In some embodiments, the agent heartbeat function also provides regular updates for information important to user service notification services. For example, the network based elements can provide regular synchronization updates for the device based service usage or service activity counters in which service usage or service activity measures available from one or more network service history elements is transmitted to the device 100. This allows the service usage counter errors between the device service counter and the counters used for central billing to be minimized. A common service usage or service activity measure is total traffic usage measured to date within a time frame over which a service limit is applicable. Other service usage or service activity measures can also be tracked and reconciled in a similar manner.

[0175] In some embodiments for the heartbeat function, the service controller 122 verifies that the scheduled agent reports are being received and that the reports are within expected parameters. In some embodiments, the access control integrity server 1654 issues signed challenge/response sequences to the policy implementation agent 1690. For example, the challenges can be asynchronous, issued when an event or error condition occurs, issued on a schedule or issued when a certain amount of data has passed. This approach, for example, provides a second layer of service policy implementation verification that strengthens the service usage or service activity measurement verification. For example, a challenge/response can be sent over the heartbeat link for the purpose of verifying device agent integrity. Various challenge/response related verification embodiments are described below.

[0176] In some embodiments, the challenge/response heartbeat message can include sending any kind of command or query, secure or transmitted in the open, receiving a response from the agent and then evaluating the response to determine if the response is within a range of parameters expected for a correctly configured agent, an agent that is operating properly, an agent that is not partially compromised or an agent that is not entirely compromised. In some embodiments, the agent is only required to respond with a simple acknowledgement of the challenge. In some embodiments, the agent is required to respond with a message or piece of information that is known by the agent. In some embodiments, the agent is required to respond with a message or piece of information that is difficult for the agent to respond correctly with if it were to be partially or entirely compromised. In some embodiments, the agent is required to respond back with information regarding the operation or configuration of the agent that is difficult for the agent to respond properly with if the agent is not properly configured, not operating properly, is partially compromised or is entirely compromised. In some embodiments, the first agent is required to respond back with information regarding the operation, configuration, status or behavior of a second agent that is difficult for the first or second agent to respond properly with if the first or second agent is not properly configured, not operating properly, is partially compromised or is entirely compromised. In some embodiments, the agent is required to respond with a response that includes a shared secret. In some embodiments, the agent is required to respond with information regarding the presence, configuration, operating characteristics or other information regarding other programs in the operating environment of the agent. In some embodiments, the agent is required to respond with hashed information to be portions of code or a code sample (e.g., the code portion or code sample can be specified by the service controller 122).

[0177] In some embodiments, the information the agent responds with is a response to a signed or encrypted message from the service controller 122 in which the agent must know how to decode the encrypted controller message in order to respond correctly or it would be difficult for the agent to respond properly if the agent is not configured properly, is not operating within appropriate limits, is partially compromised or is entirely compromised. In some embodiments, the agent signs or encrypts information in such a manner that it is difficult to respond correctly when the message is decoded by the service controller 122 unless the agent is configured properly, is operating within appropriate limits, is not partially compromised and is not entirely

compromised. In some embodiments, the agent is required to respond with a signed or encrypted hash of information that is difficult for the agent to generate unless the agent is configured properly, is operating within appropriate limits, is not partially compromised and is not entirely compromised. For example, the hashed information can be local device configuration information, portions of code or all of the code, and/or the code portion to be used in the response can be specified by the service controller. In another example, the hashed information the agent responds with can include a shared secret, and/or the hashed information can be information regarding the presence, configuration, operating characteristics or other information regarding other programs in the operating environment of the agent.

[0178] Accordingly, as described above, the agent heartbeat function provides an important and efficient system in some embodiments for verifying the service policy implementation or protecting against compromise events. For example, there are many other functions the agent heartbeat service can perform and some are described herein while others will be apparent to one of ordinary skill in the art given the principles, design background and various embodiments provided herein.

[0179] In some embodiments, the service control device link 1691 facilitates another important function, which is the download of new service processor software elements, revisions of service processor software elements, and/or dynamic refreshes of service processor software elements. There are many embodiments for such operations. In some embodiments, the software is received as a single file over the service control device link 1691. For example, the file can have encryption or signed encryption beyond any provided by the communication link protocol itself. In some embodiments, the software files are segmented into smaller packets that are communicated in multiple messages sent over the service control device link 1691. In some embodiments, once the file(s) are received, or the segmented portions of the file(s) are received, they are communicated to a service downloader 1663 for file aggregation and installation, which, in some embodiments, is performed after further measures to verify the service processor software are completed. In some embodiments, the files are sent using other delivery means, such a direct TCP socket connection to the service downloader 1663 or some other software installer, which can also involve secure transport and additional levels of encryption.

[0180] As shown in FIG. 16, an agent communication bus 1630 represents a functional description for providing communication for the various service processor 115 agents and functions. In some embodiments, as represented in the functional diagram illustrated in FIG. 16, the architecture of the bus is generally multipoint to multipoint so that any agent can communicate with any other agent, the service controller or in some cases other components of the device, such user interface 1697 and/or modem components. As described below, the architecture can also be point to point for certain agents or communication transactions, or point to multipoint within the agent framework so that all agent communication can be concentrated, or secured, or controlled, or restricted, or logged or reported. In some embodiments, the agent communication bus is secured, signed, encrypted, hidden, partitioned and/or otherwise protected from unauthorized monitoring or usage.

[0181] In some embodiments, as described below, there are multiple layers of security applied to the agent communication bus 1630 communication protocols, such as including one or more of the following: point to point message exchange encryption using one or more keys that are partially shared or shared within the service processor 115 agent group and/or the service controller 122, point to point message exchange that using one or more keys that are private to the two endpoints of the communication, a bus-level message exchange encryption that can be in place of or in addition to other encryption or security, or using one or more keys that are partially shared or shared within the service processor 115 agent group and/or the service controller 122, a set of secure messages that can only be decoded or observed by the agents they are intended for, a set of secure messages that allow communication between certain agents or service processor functions and entities outside of the service processor operating environment. In some embodiments, and as described herein, the service control device link 1691 is assumed to be equivalent to an agent for communication purposes, and, in the case of the service control device link 1691, the communication is not restricted to the agent communication bus 1630 but also extends to the service control communications link 1653. In some embodiments, the system has the capability to replace keys or signatures on occasion or on a regular basis to further secure against monitoring, eavesdropping or compromise of the agent communication system.

[0182] For example, various forms of message encryption and security framework techniques can be applied to encrypt and/or secure the agent communication bus 1630, including

one or more of the following: agent bus encryption using shared key for all agents provided and updated by the secure server; agent bus encryption using point to point keys in which the secure server informs the bus and agents of keys and updates as appropriate; agent level encryption using agent to agent shared keys in which the secure server informs agents of the key and updates the key as appropriate; agent level encryption using agent to agent point to point key in which the secure server informs agent of the point to point keys that are required and updates the keys as appropriate; agent level access authorization, which only allows access to the agents that are on the secure authorization list and in which the list is provided by the secure server and signatures are provided by the secure server; UI messages are only analyzed and passed, in which the UI cannot have access to configuration information and cannot issue challenges; agent level heartbeat encryption, which can be point to point or shared key for that agent; control link level heartbeat encryption; TLS (Transport Layer Security) communication protocols; server level heartbeat encryption, which can be point to point or shared key for that secure server; and/or the access control integrity agent 1694 or heartbeat function can become point to multipoint secure communications hubs.

[0183] In some embodiments of the agent communication bus 1630, the design of the agent communication bus depends on the nature of the design embodiments for the agents and/or other functions. For example, if the agents are implemented largely or entirely in software, then the agent communication bus can be implemented as an inter-process software communication bus. In some embodiments, such an inter-process software communication bus is a variant of D-bus (e.g., a message bus system for inter-process software communication that, for example, helps applications/agents to talk to one another), or another inter-process communication protocol or system, running a session bus in which all communications over the session bus can be secured, signed, encrypted or otherwise protected. For example, the session bus can be further protected by storing all software (e.g., software components, applications and/or agents) in secure memory, storing all software in encrypted form in secure memory, and/or executing all software and communications within a secure execution environment, hardware environment and/or protected memory space. In some embodiments, if the agents and other functions are designed with a mixture of software and hardware, or primarily with hardware, then the implementation of the bus design will vary, and the principles and embodiments described herein

will enable one of ordinary skill in the art to design the specifics of the agent communication bus 1630 to meet a particular set of product and desired functional requirements.

[0184] As shown in FIG. 16, an access control integrity agent 1694 collects device information on service policy, service usage or service activity, agent configuration and agent behavior. In some embodiments, the access control integrity agent 1694 also cross checks this information to identify integrity breaches in the service policy implementation and control system. In some embodiments, the access control integrity agent 1694 also initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, the access control integrity agent 1694 also performs asynchronous or periodic agent checks to verify presence, configuration or proper operation of other agents. In some embodiments, the access control integrity agent 1694 also performs challenge-response sequence verification of other agents.

[0185] In some embodiments, the access control integrity agent 1694 obtains service usage or service activity measures from a service monitor agent 1696 and compares one or more first service usage measurement points against one or more second service usage measurement points to verify service policy implementation. For example, as shown in FIG. 21, if the service usage at measurement point IV is inconsistent with measurement point III, which, for example, can indicate, for example, that an unauthorized or unmonitored usage of the access modem (e.g., modems 2122, 2123, 2124, 2125 or 2141) is taking place. As another example, as also shown in FIG. 21, if one or more aspects of upstream traffic usage measurement point II, which represents the upstream demand side of policy implementation agent 1690, is inconsistent with upstream traffic measurement point III, which represents delivered traffic from the policy implementation agent 1690, then the policy implementation agent 1690 may not be operating properly. As another example, as also shown in FIG. 21, if service measurement point III and IV indicate that firewall agent 1655 is passing traffic to URLs or IP addresses that are in the blocked policy settings, then a verification error condition can be set for the access control policy. As another example, if the policy controller reports traffic usage statistics that are inconsistent with traffic usage policy settings, then a traffic usage policy verification error may have occurred. As another example, if the service usage counter synchronization information received from the service controller 122, the device service history 1618 and/or the central billing system 1619, is

compared to the service usage history reported by the service monitor agent and the two are found to be outside of acceptable tolerance limits for the comparison, then there may be a verification error in the service monitor service usage or service activity accounting. There are numerous additional embodiments of such comparisons as described herein and others as will be readily apparent to one of ordinary skill in the art given the principles, design background and specific examples and various embodiments described herein.

[0186] In some embodiments, device service policy implementations are verified by comparing various service usage measures used at the device against expected service usage or service activity behavior given the policies (e.g., one or more service policy settings, service profile or service profile settings for network based access/services, and/or service plan or service plan for network based access/services). For example, verification is performed based on a measure of total data passed at the device as compared to the service policy for total data usage. For example, verification is performed based on a measure of data passed in a period of time at the device as compared to the service policy for data passed in such a period of time. For example, verification is performed based on a monitoring of communications from the device based on IP addresses as compared to the policy for permissible IP addresses. For example, verification is performed based on a measure of total data passed from the device per IP address as compared to the policy for total data usage per IP address. Other examples include such actual versus policy comparisons based on other measures at/from/to the device, such as location, downloads, email accessed, URLs, and/or any other data, location, application, time or other criteria or any combination of criteria that can be measured for comparing with various policy settings and/or restrictions.

[0187] In some embodiments, the access control integrity agent 1694 monitors agent self-check reports to verify that agents are properly configured. In some embodiments, the access control integrity agent 1694 reports the agent self check reports to the service controller 122. In some embodiments, the access control integrity agent 1694 performs a role in service usage test transmission, reception and/or monitoring, with the usage test being tailored to test monitoring or control aspects for any subset of service activities. In some embodiments, the access control integrity agent 1694 performs a role in billing test event generation and/or monitoring. In some embodiments, the access control integrity agent 1694 checks and reports the result of service

usage monitoring verification tests, service usage billing verification tests and/or transaction billing verification tests.

[0188] In some embodiments, the access control integrity agent 1694 receives agent access attempt reports to determine if unauthorized agent access attempts are occurring. In some embodiments, the access control integrity agent 1694 acts as a central secure communications hub for agent to agent or service controller 122 to agent communication. For example, the access control integrity agent 1694 can be used so that no other software or function can access other agents or so that agents cannot access other agents except through the secure point to multipoint communications hub. In some embodiments, this approach further enhances compromise resistance for the agents. In some embodiments, some or all of the agent communications, including agent to agent or service controller 122 to agent communications, and possibly including unauthorized attempts to communication with agents, are monitored and logged so that a trace log of some or all agent communications can be maintained. For example, the agent communication trace log can be summarized and/or compressed for transmission efficiency or regularly reported, such as through the heartbeat function, or the agent communication trace log can be reported only when the service controller 122 requests the agent communication trace log or when there is a verification error event. As similarly described above, the partitioning of agent functions and server functions is provided herein mainly to aid in disclosing various embodiments but those of ordinary skill in the art will appreciate that other partitioning of agent functions and server functions can be used based on different design choices. For example, the central agent communication hub function is performed in some embodiments by the access control integrity agent 1694, however, in other embodiments that function is performed by the service control device link 1691. For example, when the central agent communication hub function is located in the service control device link 1691, then architecturally the device link can be a single point to multipoint secure communications hub for all agent to agent and service controller 122 to agent communications. In some embodiments, this approach has certain advantages from a service policy implementation verification or compromise protection robustness perspective, or has certain advantages from a communications protocol efficiency perspective, or simply can be more efficient to implement. It should be noted that in other embodiments described herein the agent to agent and agent to service controller 122 communications can be multipoint to multipoint, with each agent having the capability to

communicate with other agents or the service controller, this communication can be secure, signed or otherwise encrypted or protected in some embodiments and in the open/clear in others. Also, as discussed in some embodiments, the agents can maintain their own communications or attempted communications log, which can then be reported to the service controller 122. In some embodiments, the agents implement restrictions on which device components or agents the agents will conduct communications with so that only agents that need to communicate with one another can do so.

[0189] In some embodiments, the service control device link 1691 reviews local billing event history and compares such history to billing event reports to verify that a billing agent 1695 is functioning properly (e.g., has not been tampered with or compromised). In some embodiments, the service control device link 1691 cross-checks service usage or service activity against billing event reports from the billing agent 1695 to verify that billing events are properly billing for service usage or service activity. In some embodiments, the service control device link 1691 cross-checks transaction billing process or records against transaction billing reports to ensure that transaction billing events are being properly reported by the billing agent 1695. In some embodiments, the service control device link 1691 determines if one or more agents have been compromised, and if so, initiates a dynamic agent download process to replace any such potentially compromised agent.

[0190] In some embodiments, the access control integrity agent 1694 verifies that the service usage counter is reporting service usage or service cost to the user within acceptable limits of accuracy when compared to the service usage reports obtained from the service monitor agent 1696, the service controller 122, the device service history 1618 and/or the central billing system 1619. In some embodiments, the access control integrity agent 1694 checks to verify that user privacy filter preferences are being properly implemented. In some embodiments, the access control integrity agent 1694 checks to verify that the user is properly receiving UI warnings regarding service usage or roaming service usage conditions.

[0191] In some embodiments, the access control integrity agent 1694 checks to verify that the device is not beginning service usage until it has been authenticated, authorized or granted access to the network. In some embodiments, access control integrity agent 1694 checks

with the service controller 122 or the billing system 1619 to verify that the user or device has a valid service standing and should be admitted to access on the network.

[0192] In some embodiments, an Activation Tracking Service (ATS) is provided in which the service monitoring function (e.g., performed by the service monitor agent 1696 and/or some other agent/component or combinations thereof on the device) is used in part to determine which access networks are being connected to and to record and/or report this information. In some embodiments, the ATS is only enabled if the device user approves reporting of access networks connected to by the user device. In some embodiments, the ATS is protected from tampering. For example, the ATS can be hardened, that is, to be more tamper resistant, using a variety of techniques, including any of the following: the ATS can be located (e.g., stored) in secure memory and/or secure hardware; the ATS can be implemented in the system BIOS, the access modem and/or another hard to access portion of the device; a second device agent can confirm the presence of the ATS with a report to a network based server; the second agent or the network server can initiate a reinstall of the ATS if it is missing or is found to be operating improperly; and/or the ATS can be placed in a secure area of the OS so that it cannot be removed or if removed must be replaced for proper device operation to resume. A variety of other tamper resistance techniques can also be used to protect the ATS from tampering as similarly described herein with respect to other device based functions/software components/agents.

[0193] In some embodiments, the access control integrity agent 1694 verifies that ATS software or hardware is present, properly configured or operating properly. In some embodiments, the access control integrity agent 1694 reviews network connection or activity history and compares such to ATS reports to verify activation tracking service reports are occurring properly. In some embodiments, the access control integrity agent 1694 replaces ATS software if it has been removed. In some embodiments, the access control integrity agent 1694 monitors access or compromise of ATS software to determine if it may have been compromised. In some embodiments, the access control integrity agent 1694 reports status of ATS functions.

[0194] In some embodiments, the access control integrity agent 1694 scans the local agent execution environment to determine if there are unauthorized accesses to service processor functions, settings or code. In some embodiments, the access control integrity agent 1694

monitors software loading activity, protected memory access or communication with service processor 115 agents to detect unauthorized changes to service processor software or configuration. For example, the access control integrity agent 1694 can have a local database of potentially malicious elements and compare entries in the database against the elements detected locally. As another example, the access control integrity agent 1694 can communicate a list of some or all of the elements detected locally to the service controller 122 to augment or take the place of the database comparison function that may be performed locally. In some embodiments, the access control integrity agent 1694 detects new software downloads, installs or invocations and immediately issues an error flag report when potentially malicious software is downloaded, installed or invoked. In some embodiments, the access control integrity agent 1694 scans the local software loading and invocation activity along with a log of other software runtime events and regularly reports this trace so that when an error or compromise event occurs the trace preceding the event can be analyzed to determine the offending software or activity trace that took place to cause the compromise or error. Once the software or activity that caused the compromise is known, it can be entered into a refreshed version of the database that the device and other devices use to detect potentially malicious pre-cursor conditions. Examples of such pre-cursor events include software invocations, software downloads, attempts to uninstall certain agent and/or application software/components or OS components, a sequence of memory I/O events, a sequence of software access events, a sequence of network address or URL communications or downloads or a sequence of access modem I/O activity. In various other embodiments of the access control integrity agent 1694, the agent performs or (securely) communicates with other software/hardware device/network components that perform other well known signature, behavior blocking and/or intrusion detection identification/detection and/or blocking techniques based on the presence of potentially unwanted and/or potentially or known malicious software and/or intrusion attempts by unauthorized software and/or unauthorized users, using, for example, real-time, on access, periodic, and/or on demand scanning.

[0195] In some embodiments, the access control integrity agent 1694 detects or blocks potentially compromising behavior of other software programs/users attempting unauthorized behavior in the service processor 115 operating environment. In some embodiments, the access control integrity agent 1694 detects software that is being loaded that has the same or similar name, identification, memory location or function as one or more of the service processor 115

agents. In some embodiments, the access control integrity agent 1694 blocks operation or loading of such software. In some embodiments, the access control integrity agent 1694 detects or blocks unauthorized access of service processor 115 protected memory. In some embodiments, the access control integrity agent 1694 verifies configuration and operation of secure service downloader 1663. In some embodiments, the access control integrity agent 1694 monitors network and I/O activity to detect potentially compromising events, such as a program that is downloaded from known detrimental or potentially suspect IP addresses or URLs or a program that accesses certain IP addresses or URLs. In some embodiments, the access control integrity agent 1694 scans of the service processor operating environment are recorded and kept for a period of time, and if a service policy verification error occurs, then the scans immediately prior to the error are analyzed or reported to the service controller 122 for analysis. In some embodiments, such scans are regularly reported to the service controller 122 without the presence of service policy verification error conditions.

[0196] In some embodiments, the access control integrity agent 1694 requests a dynamic agent download of certain critical service processor functions, including in some cases the access control integrity agent 1694 on a periodic basis, or on a periodic basis when network access activity is not required or minimal.

[0197] In some embodiments, the access control integrity agent 1694 determines if a threshold has been surpassed for a max usage trigger for ambient and/or other services that should not be using significant amounts of data (e.g., based on the type of device and/or service profile settings).

[0198] In some embodiments, the access control integrity agent 1694 determines if verification errors exist in one or more of the verification process embodiments and, in some embodiments, reports errors immediately or in the next agent heartbeat to the service controller 122. In some embodiments, any number of results from the above checks, monitoring activities, reports or tests are reported to the service controller 122.

[0199] In some embodiments, a policy control agent 1692 receives policy instructions from the service controller 122 and/or the user via the billing agent 1695 and adapts device service policy settings (e.g., instantaneous device service policy settings) in one or more of the

following agents/components: a policy implementation agent 1690, the modem firewall 1655 and/or an application interface agent 1693. As shown in FIG. 16, the modem firewall 1655 is in communication with a modem driver 1640, which is in communication with the agent communication bus 1630 and access network 1610. As shown with respect to access network 1610, a central billing server 1619, an access network AAA server 1621 and device server history 1618 are also provided. As shown, the Internet 120 is accessible via the access network 1610 and firewall 124, from which device 100 can then access various Internet services 1615.

[0200] In some embodiments, the policy control agent 1692 adapts low level service policy rules/settings to perform one or more of the following objectives: achieve higher level service usage or cost objectives, reduce network control channel capacity drain, reduce network control plane server processing bandwidth, and/or provide a higher level of user privacy or network neutrality while satisfying service usage or service activity objectives. In some embodiments, the policy control agent 1692 performs a policy control function to adapt instantaneous service policies to achieve a service usage objective. In some embodiments, the policy control agent 1692 receives service usage information from the service monitor agent 1696 to evaluate service usage history as compared to service usage goals. In some embodiments, the policy control agent 1692 uses service monitor 1696 service usage or service activity history and various possible algorithm embodiments to create an estimate of the future projected service usage. In some embodiments, the policy control agent 1692 uses a future projection of service usage to determine what service usage or service activity controls need to be changed to maintain service usage goals. In some embodiments, the policy control agent 1692 uses service usage history to perform a service usage or service activity analysis to determine the distribution of service usage across service usage elements within categories, such as usage by application, usage by URL, usage by address, usage by content type, usage by time of day, usage by access network, usage by location, and/or any other categories for classifying service usage. In some embodiments, the policy control agent 1692 uses the service usage distribution analysis to determine which service usage elements or service activities are creating the largest service usage (e.g., if e-mail, social networking, or multimedia/online video application categories are creating the largest service usage).

[0201] In some embodiments, the policy control agent 1692 is instructed, for example, by the user, through billing agent 1695 to perform a service control algorithm, such as traffic shaping or download management, to manage service usage or service activities to assist the user in controlling service costs. As a basic example of such a traffic shaping algorithm, the traffic shaping algorithm can simply reduce traffic speed for all applications and traffic types successively until the service usage projections are within service usage limits for the present service billing period. To illustrate an algorithm that is more sophisticated and provides the advantage of leaving many service usage elements or service activities unaffected while only controlling down usage on the most aggressive service usage elements or service activities, the traffic shaping algorithm can identify the highest traffic usage applications and/or websites and successively reduce traffic speed just for the highest usage applications and/or websites until the service usage projections are within service usage limits for the present service billing period. These examples thereby reduce network traffic for the user in accordance with the user's service usage objectives while maintaining overall satisfactory service usage experience for the user in a manner that satisfies various net neutrality requirements (e.g., the traffic throttling of certain applications/websites based on user input in which categories based on service usage history are selected by the user, for example, a certain application may be using 90% of the aggregate traffic usage). For example, adaptive throttling algorithms can be used to throttle application traffic that the user requests throttling, such as recursively throttling of the specified application traffic (e.g., to denigrate the traffic usage associated with that application and thereby reduce overall service data usage).

[0202] In some embodiments, the policy control agent 1692 adjusts service policy based on time of day. In some embodiments, the policy control agent 1692 obtains a measure of network availability and adjusts traffic shaping policy settings based on available network capacity. In some embodiments, the policy control agent 1692 automatically and dynamically adjusts service policy based on one or more other service policy settings, the service profile and/or the service plan associated with the device and/or user of the device.

[0203] In some embodiments, various lower level service policy implementation embodiments are combined with a higher level set of service policy supervision functions to

provide device assisted verifiable network access control, authentication and authorization services.

[0204] In some embodiments, device based access control services are extended and combined with other policy design techniques to create a simplified device activation process and connected user experience referred to herein as ambient activation. In some embodiments, ambient access generally refers to an initial service access in which such service access is in some manner limited, such as where service options are significantly limited (e.g., low bandwidth network browsing and/or access to a specific transactional service), limited bandwidth, limited duration access before which a service plan must be purchased to maintain service or have service suspended/disabled or throttled or otherwise limited/reduced/downgraded, and/or any other time based, quality based, scope of service limited initial access for the network enabled device. In some embodiments, ambient activation is provided by setting access control to a fixed destination (e.g., providing access to a portal, such as a web page (e.g., for a hotspot) or WAP (Wireless Application Protocol) page, that provides the user with service plan options for obtaining a service plan for the user desired access, such as the service plan options for data usage, service types, time period for access (e.g., a day pass, a week pass or some other duration), and costs of service plan(s)). In some embodiments, service data usage of the ambient activated device is verified using IPDRs (e.g., using the device ID/device number for the device 100 to determine if the device has been used in a manner that is out of plan for the service plan associated with the device 100, such as based on the amount of data usage exceeding the service plan's service data usage limits, out of plan/unauthorized access to certain websites, and/or out of plan/unauthorized transactions). In some embodiments, service data usage of the ambient activated device is verified by setting a maximum data rate in the policy control agent 1692 and if/when it is determined that the device is exceeding a specified data rate/data usage, then the service data usage is throttled accordingly. In some embodiments, various other verification approaches are used for ambient activation purposes.

[0205] In some embodiments, the policy control agent 1692 (and/or another agent/component of the service processor 115 and/or service controller 122) performs a service control algorithm to assist in managing overall network capacity or application QoS (Quality of Service). In some embodiments, the policy control agent 1692 (and/or another agent/component

of the service processor 115) performs an access network selection algorithm to determine which access network to connect to based on connection options and determined strengths of available wireless networks, network preference or security settings, service usage cost based network preferences, and/or any other criteria.

[0206] Accordingly, as described herein with respect to various embodiments, service usage or service activities can be measured by various agents at various different measurement points, which provides for a more robust verification and integrity of device based services communication. For example, it is much less likely and more difficult to compromise and/or spoof multiple agents. As described herein, various verification and integrity checks are performed, including, for example, network based service usage measurement (e.g., using IPDRs); heartbeat monitoring; agent based heartbeat (e.g., challenge/response queries); agent operating environment protection; monitoring agent communications; agent cross-checks; comparing device based and network based measures (e.g., service usage measures); dynamic software/agent download; and/or any combination of these and various other verification/integrity check techniques described herein and/or apparent from the various embodiments described herein.

[0207] In some embodiments, the device 100 is capable of connecting to more than one network and device service policies are potentially changed based on which network the device is connected to at the time. In some embodiments, the network control plane servers detect a network connection change and initiate the service policy implementation established for the second network. In some embodiments, the device based adaptive policy control agent, as described herein (e.g., policy control agent 1692), detects network connection changes and implements the service policies established for the second network.

[0208] In some embodiments, when more than one access network is available, the network is chosen based on which network is most preferred according to a network preference list or according to which network that optimizes a network cost function. For example, the network preference list can be pre-established by the service provide and/or the user and/or later modified/adjusted by either the service provider and/or the user. For example, the cost function can be based on determining a minimum service cost, maximum network performance, whether

or not the user or device has access to the network, maximizing service provider connection benefit, reducing connections to alternative paid service providers, and/or any other cost related criteria for network selection purposes.

[0209] In some embodiments, the device 100 detects when one or more preferred networks are not available, implements a network selection function or intercepts other network selection functions, and offers a connection to the available service network that is highest on a preference list. For example, the preference list can be set by the service provider, the user and/or the service subscriber. In some embodiments, a notification is provided to the device/user when the device is not connected to a network (e.g., indicating in a pop-up/bubble or other UI based display a notification, such as “You are not connected to the network. Click here to learn more, get free trial, use a session, sign-up for service”). In some embodiments, the notification content can be determined based on usage service patterns, locally stored and/or programmable logic on the device and/or a server (e.g., device reports that user is not connected and WWAN is available). Decisions on what bubble to present when may be in pre-stored logic on device.

[0210] In some embodiments, service policies are automatically adapted based on the network to which device 100 is connected. For example, the device can be a cellular communication based device connected to a macrocell, a microcell, a picocell, or a femtocell (e.g., femto cells generally provide a low power, small area cellular network used, for example, in homes or offices, which, for example, can be used as an alternative to Wi-Fi access). In some embodiments, service monitoring agent 1696 and/or billing agent 1695 modify service usage counting and/or billing based on whether the device is connected to a macrocell, microcell, picocell or femtocell. In some embodiments, the device recognizes which type of network it is currently connecting to (e.g., looking up in a local or network table for the current base station connected to, and/or the information is broadcast to the device upon the connection with the base station), that is, whether it is a macrocell, microcell, picocell or femtocell. In other embodiments, the device does not recognize which type of network it is currently connected to, but reports its current base station, and the network uses a network lookup function to determine which type of network it is connected to. In some embodiments, the device adjusts the billing based on the type of network it is connected to, or in other embodiments, the device calculates an offset to such billing based on the type of network it is connected to, and/or in other

embodiments, the device records such service usage associated with the type of network it is connected to and the network billing can adjust the billing accordingly. For example, the billing can be lower for service data usage over a femtocell versus a macrocell. In some embodiments, service policies are adjusted based on the type of network that the device is connected, such as billing, user notification, data usage/bandwidth, throttling, time of day, who owns the cellular network connection (e.g., user's home femtocell, or user's work femtocell, or a commercial business's femtocell like a coffee shop or any other common area like an airport) and/or any other service policy can be different for a femtocell connection (or for any other type of connection, such as a macrocell, microcell, or picocell). In some embodiments, the local service usage counter is adjusted based on the type of network (and/or based on the time of day of such service activity) that the device is connected, such as billing, user notification, data usage/bandwidth, and/or any other service policy can be different for a femtocell connection (or for any other type of connection, such as a macrocell, microcell, or picocell). In some embodiments, the service policies and/or billing policies are adjusted based on network congestion.

[0211] In some embodiments, if adaptive service policy control is not required, then the policy control agent 1692 can simply pass instantaneous service policy settings directly to the agents responsible for implementing instantaneous service policies.

[0212] In some embodiments, a policy implementation agent 1690 implements traffic shaping and QoS policy rules for the device 100. In some embodiments, the policy implementation agent 1690 provides a firewall function. In some embodiments, the policy implementation agent 1690 performs traffic inspection and characterization. In some embodiments, packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed entirely in/by the policy implementation agent 1690. In some embodiments, the policy implementation agent 1690 accepts service policy implementation settings from the policy control agent 1692 or directly from the service controller 122. More detail on specific embodiments for the policy implementation agent 1690 is provided below with respect to the figures associated with communication stack and communication protocol flow.

[0213] In some embodiments, the burst size, buffer delay, acknowledgement delay and drop rate used in upstream and downstream traffic shaping are optimized with the goal of reducing access network traffic overhead, and excess capacity usage that can result from mismatches in traffic transmission parameters with the access network MAC and PHY or from excess network level packet delivery protocol re-transmissions. In some embodiments, the application interface agent 1693 is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. As shown in FIG. 16, the application interface agent 1693 is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[0214] In some embodiments, downstream literal or virtual application tagging are delayed until a traffic flow passes through the service policy implementation functions and to the application interface function where the service flow is then identified and associated with the underlying traffic and application parameters, and the literal or virtual tag is then communicated to the first policy implementation function or service monitoring function in the downstream traffic processing stack. In some embodiments, prior to being associated with a literal or virtual tag, the traffic flow is allowed to pass with no traffic shaping, and once the traffic flow is identified and tagged, the appropriate traffic shaping is applied. In some embodiments, a set of traffic shaping policy parameters are applied to the unidentified traffic flow before the flow is identified, and then the traffic shaping policy for the flow is updated when the flow is tagged. In some embodiments, the traffic flow can be blocked at the application interface agent even before the tag is passed to the policy implementation functions if it is found to be associated with traffic parameters that are blocked by policy once packet processing, framing and encryption are removed.

[0215] In some embodiments, a service monitor agent 1696 records and reports device service usage or service activities of device 100. In some embodiments, service usage history is verified by a number of techniques including verifying against network based service usage history (e.g., device service history 1618) and the various service policy implementation techniques as described herein.

[0216] In some embodiments, the service monitor agent 1696 includes the capability to filter service usage history reporting with the decision on which aspects of service history to report being determined by policies including possibly privacy policies defined by the device user or control plane servers in the network. In some embodiments, the service monitor agent 1696 monitors and possibly records or reports Customer Resource Management (CRM) information such as websites visited, time spent per website, interest indications based on website viewing, advertisements served to the device, advertisements opened by the user, location of the user, searches conducted by the user, application usage profile, device user interface usage history, electronic commerce transactions, music or video files played, applications on device, and/or when the user is actively working or playing or inactive. In some embodiments, to protect the privacy of this user CRM information, the user is provided with options on how much of the information to share and the user's response to the options are recorded and used to determine the filtering policy for how much of the CRM data to report (e.g., CRM filter level options selected by the user via the device UI and/or via various service plan or service profile or service policy options) and how much to suppress or to not even monitor/record/store in the first place. In some embodiments, to protect the privacy of this user's GPS/location tracking related information, the user is provided with options on how much of the information to share and the user's response to the options are recorded and used to determine the filtering policy for how much of the GPS/location tracking related data to report (e.g., GPS/location tracking filter level options) and how much to suppress or to not even monitor/record/store in the first place. In some embodiments, the service processor 115 allows the user to provide feedback on the user's preferences, such as for privacy/CRM data to report. In some embodiments, the user can also specify their preference(s) for notification (e.g., related to service usage/cost, traffic reporting and other service usage/monitored information) and/or service controls. In some embodiments, the service monitor agent 1696 observes and possibly records or reports service usage categorized by network possibly including roaming networks, paid service networks or free service networks. In some embodiments, the service monitor agent 1696 observes and possibly records or reports service usage categorized by sub-accounts for various types of traffic or various types of network.

[0217] For example, service monitor reports can be provided to the service controller 122. Service is monitored through various embodiments that can involve service usage logging

or traffic inspection and usage logging at the application level, various levels in the networking communication stack or the access modem. Some embodiments involve multiple levels of service or traffic measurement at various levels in the communications stack as described further below.

[0218] In some embodiments, service or traffic monitoring includes monitoring one or more of the following: traffic associated with one or more users; traffic downstream and/or upstream data rate; total traffic received and/or transmitted over a period of time; traffic transmitted and/or received by IP addresses, domain names, URLs or other network address identifiers; traffic transmitted and/or received by email downloads or uploads; traffic transmitted and/or received by an application; traffic transmitted and/or received by network file transfers; traffic transmitted and/or received by file download or upload content types; traffic transmitted and/or received by mobile commerce transactions; traffic transmitted and/or received by one or more time periods; traffic transmitted and/or received by differing levels of network activity and network capacity availability; traffic transmitted and/or received by one or more delivered levels of quality of service; traffic transmitted and/or received by software downloads; traffic transmitted and/or received by application downloads; traffic transmitted and/or received by one or more activities associated with the service control plane link or other network related functions, or traffic that may not directly result in service usage or service activity that the user values or desires; traffic transmitted and/or received to support one or more service provider third party service partner offerings; software usage history; application usage history; device discovery history for UI components, applications, settings, tutorials; ads served history; ads visited history; and/or device location history.

[0219] In some embodiments, some or all of the service usage monitoring occurs at the application layer. In some embodiments, the service monitor agent 1696 implements traffic inspection points between the applications and the networking stack application interface, such as the sockets API. In other embodiments, the application interface agent 1693 performs traffic inspection and reports the results to the service monitor agent 1696. Traffic inspection can be accomplished in several ways, including, for example, implementing a T-buffer at each socket connection and feeding the side traffic into a traffic flow analyzer, which in combination with a mapping of application to socket provides much of the information listed above. In cases in

which it is necessary to obtain traffic information from the application itself, some embodiments call for the application to be adapted to provide the information to either the application interface agent 1693 or the service monitor agent 1696. As an example, the application interface agent 1693 or the service monitor agent 1696 can monitor and decode advertisements downloaded via HTTP, but if the browser and HTTP server employ security above the sockets protocol stack layer then the application interface agent can communicate with the browser via a java applet or some other inter-process communication method. In some embodiments, the service monitor agent 1696, the billing agent 1695 and/or the policy control agent 1692 (or some other software or hardware function on the device) can monitor and/or control (e.g., allow, block and/or replace) advertisement traffic flow into the device. In some embodiments, the monitoring and control of advertisement traffic flow into the device is also used for bill by account purposes (e.g., charges, such as service charges, billed to the advertiser, sponsor, and/or service or transactional service provider).

[0220] In some embodiments, some or all of the service usage monitoring occurs below the application interface for the networking stack. In this case, some portion of the information listed above may not always be available due to encryption applied at the higher layers and/or the computational costs associated with performing deep packet inspection on mobile devices.

[0221] In some embodiments, the service monitor agent 1696 is also monitors the operating software install or loading systems, and/or otherwise monitors software installs or loads and/or software uninstalls/deinstallations.

[0222] Some of the information above may be considered by some users, advocacy groups or agencies as customer sensitive personal information. Simply sending the above information to the network for unspecified purposes may not, therefore, be acceptable for some service providers. However, if the user provides specific approval (e.g., informed consent) for the device, network or service provider to use some or all of the information that may be sensitive for specified purposes, then the user can control the level of information that is used and the purpose the information is used for. Accordingly, various embodiments described herein provide the user with control of what information is used and the purposes it is used for thereby allowing the user adequate control of any such sensitive information. In some embodiments,

information that is thought to perhaps be sensitive and is reported to the network must first receive user approval for the reporting. Some basic information is generally not considered sensitive and is necessary for certain basic service provider needs. For example, total data transmitted and/or received, traffic downstream and/or upstream speed, overall traffic usage by time of day are generally not considered private from the service provider's perspective and are necessary in many basic service policy implementations. As additional examples, perhaps other service usage history, such as total traffic email downloads and uploads but not the type of files or any specifics about the email traffic, the total web browsing traffic but nothing specific about the sites visited or content viewed, total file transfer traffic but not the type of files transferred or the addresses involved in the transfer, and other examples may not be viewed as private and, in some embodiments, provide valuable information for the service provider to manage services. Conversely, information such as websites visited, content viewed, mobile commerce transactions completed, advertisements visited, GPS location history and other service usage history the service monitor is capable of recording may be sensitive or private for some users and would thereby benefit from the various embodiments that provide enhanced user control of the reporting of such potentially sensitive or private data. It should also be appreciated that there is an inherent advantage to implementing traffic monitoring, traffic, service monitoring or service control on a device, because it is not necessary to report sensitive information to the network to accomplish many of these service policy implementation objectives.

[0223] In some embodiments, the service monitor agent 1696 assists in virtual application tagging of traffic flows through the networking stack policy implementation by tracking the virtually tagged packets through the stack processing and communicating the flow tags to the service policy implementation agent(s) 1690. In some embodiments, the service monitor agent 1696 maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the service controller 122 to which the device has connected. In some embodiments, this network activity summary includes a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. In some embodiments, the traffic reports that go to the network, possibly to service controller 122, billing system 1619 and/or device service history 1618, are first filtered according to rules defined by user preference selection at the time of service activation (e.g., service plan/service plan option selection), time of first device use, at a time the user selected the option on the

service UI or at a time the user chose to change the option on the service UI or some other time/mechanism allowing for user preference selection.

[0224] In some embodiments, the service monitor agent 1696 monitors application usage (e.g., which application the user executes on the device 100, such as e-mail applications, web browsing applications and/or media content streaming applications). In some embodiments, the service monitor agent 1696 monitors multimedia file usage (e.g., based on multimedia file type and/or based on specific multimedia files, such as specific movies and/or songs). In some embodiments, the service monitor agent 1696 monitors the device user interface, application, and content discovery history (e.g., monitoring which applications/content the user accesses from the device, including monitoring the pattern by which the user accesses such applications/content, such as how the user navigates the user interface on the device to access such applications/content and maintaining such patterns and history, such as which icons the user access on a home page, secondary or other portion/mechanism on the device for accessing various applications/content). In some embodiments, the service monitor agent 1696 monitors advertisements provided to the user on the device 100. In some embodiments, the service monitor agent 1696 monitors advertisements viewed (e.g., accessed, such as by clicking on a web advertisement) by the user on the device 100. In some embodiments, the service monitor agent 1696 monitors GPS/location information for the device 100. As will be appreciated by those of ordinary skill in the art, the service monitor agent 1696 can monitor a wide variety of activities performed by the device/user of the device and/or based on other information related to the device 100 such as GPS/location information. As described herein, in some embodiments, the user of the device 100 can also specify which activities that the user authorizes for such monitoring (e.g., the user may prefer to not allow for such GPS/location monitoring).

[0225] In some embodiments, the application interface agent 1693 provides an interface for device application programs. In some embodiments, the application interface agent 1693 identifies application level traffic, reports virtual service identification tags or appends literal service identification tags to assist service policy implementation, such as access control, traffic shaping QoS control, service type dependent billing or other service control or implementation functions. In some embodiments, the application interface agent 1693 assists with application layer service usage monitoring by, for example, passively inspecting and logging traffic or

service characteristics at a point in the software stack between the applications and the standard networking stack application interface, such as the sockets API. In some embodiments, the application interface agent 1693 intercepts traffic between the applications and the standard network stack interface API in order to more deeply inspect the traffic, modify the traffic or shape the traffic (e.g., thereby not requiring any modification of the device networking/communication stack of the device OS). In some embodiments, the application interface agent 1693 implements certain aspects of service policies, such as application level access control, application associated billing, application layer service monitoring or reporting, application layer based traffic shaping, service type dependent billing, or other service control or implementation functions.

[0226] In some embodiments, application layer based traffic monitoring and shaping can be performed as described below. The traffic from each application can be divided into one or more traffic flows that each flow through a traffic queue, with each queue being associated with one or more additional classifications for that application (e.g., the application can be a browser that is associated with multiple queues representing different destinations or groups of destinations it is connected to, with each destination or group of destinations having potentially different access control or traffic control policies, or the application can be associated with different content types or groups of content types with each content type having different queues, the application might be an email program with email text traffic going to one queue and downloads going to another with different policies for each). In some embodiments, queues are formed for all applications or groups of applications that are associated with one or more traffic parameters such as destination, content type, time of day or groups of applications can be similarly assigned to different queues. The functions performed by the application layer queues can be similar to the functions described for the policy implementation agent, such as pass, block, buffer, delay, burst in order to control the traffic or network access associated with the queue. The drop function can also be implemented, such as for application layer protocols that include reliable transmission methods, but if the application layer protocol does not involve reliable retransmission of lost information this can result in lost data or unreliable communication which may be acceptable in some cases. The manner in which the queues are controlled can be constructed to result in a similar approach for controlling services or implementing service activity control similar to the other embodiments described herein,

including, for example, the policy control agent 1692 implementing an higher layer of service control to achieve a higher level objective as discussed herein.

[0227] In some embodiments, the application interface agent 1693 interacts with application programs to arrange application settings to aid in implementing application level service policy implementation or billing, such as email file transfer options, peer to peer networking file transfer options, media content resolution or compression settings and/or inserting or modifying browser headers. In some embodiments, the application interface agent 1693 intercepts certain application traffic to modify traffic application layer parameters, such as email file transfer options or browser headers. In some embodiments, the application interface agent 1693 transmits or receives a service usage test element to aid in verifying service policy implementation, service monitoring or service billing. In some embodiments, the application interface agent 1693 performs a transaction billing intercept function to aid the billing agent 1695 in transaction billing. In some embodiments, the application interface agent 1693 transmits or receives a billing test element to aid in verifying transaction billing or service billing.

[0228] In some embodiments, a modem firewall 1655 blocks or passes traffic based on service policies and traffic attributes. In some embodiments, the modem firewall 1655 assists in virtual or literal upstream traffic flow tagging. Although not shown in FIG. 16, in some embodiments, the modem firewall 1655 is located on either side of the modem bus and in some embodiments it is advantageous to locate it on the modem itself.

[0229] In some embodiments, the billing agent 1695 detects and reports service billing events. In some embodiments, the billing agent 1695 plays a key role in transaction billing. In some embodiments, the billing agent 1695 performs one or more of the following functions: provides the user with service plan options, accepts service plan selections, provides options on service usage notification policies, accepts user preference specifications on service usage notification policies, provides notification on service usage levels, provides alerts when service usage threatens to go over plan limits or to generate excess cost, provides options on service usage control policy, accepts choices on service usage control policy, informs policy control agent 1692 of user preference on service usage control policy, provides billing transaction options and/or accepts billing transaction choices. In some embodiments, the billing agent 1695

interacts with transaction servers (e.g., open content transaction partner sites 134) to conduct ecommerce transactions with central billing 1619.

[0230] In some embodiments, service processor 115 includes one or more service usage or service activity counters. For example, the service monitor agent 1696, billing agent 1695 or a combination of these agents and/or other agents/components of service processor 115 can include such a local service usage counter(s) for the device 100. In some embodiments, a service usage counter monitors service usage including data usage to/from the device 100 with the access network 1610. In some embodiments, the service usage counter periodically, in response to a user request, in response to a service processor 115 agent's request (e.g., the billing agent 1695, the policy control agent 1692, or another agent of service processor 115), in response to the service controller 122, and/or in response to the central billing 1619 (e.g., for billing purposes and/or for storing in the device service history 1618), provides a service usage report, including monitored service usage for the device 100. In some embodiments, the service usage counter periodically, or in response to a request, synchronizes the service usage counter on the device 100 with a network (and/or billing) service usage counter, such as that maintained potentially at central billing 1619. In some embodiments, service processor 115 utilizes the service usage counter to provide a service usage projection. In some embodiments, service processor 115 utilizes the service usage counter to provide a service usage cost estimate. In some embodiments, service usage projections from policy control agent 1692 are used to estimate the projected future service usage if user service usage behavior remains consistent. In some embodiments, service processor 115 utilizes the service usage counter to provide a cost of service usage, and the service processor 115 then periodically, or in response to a request, synchronizes the cost of service usage with, for example, the central billing 1619. In some embodiments, the service processor 115 utilizes the service usage counter to determine whether the user is exceeding and/or is projected to exceed their current service plan for data usage, and then various actions can be performed as similarly described herein to allow the user to modify their service plan and/or modify (e.g., throttle) their network data usage. In some embodiments, the service usage counter can support providing to the user the following service usage related data/reports: service usage, known usage and estimated usage, projected usage, present costs, projected costs, cost to roam, cost to roam options, and/or projected roaming costs. For example, including a local service data usage counter on the device 100 allows the service processor 115

to more accurately monitor service data usage, because, for example, network (and/or billing) service usage counters may not accurately also include, for example, control plane data traffic sent to/from the device 100 in their monitored service data usage count.

[0231] In some embodiments, verifiable device based service billing solutions are provided. For example, as described herein, various device based service billing solutions can include a wide range of verification techniques to ensure that the device is properly reporting service billing events (e.g., to verify/ensure that the service billing is not malfunctioning and/or has not been tampered with/compromised such that it is not accurately or timely providing service billing information). As described herein, service billing generally refers the billing for one or more services for a device, such as device 100 (e.g., email service billing for data usage associated with received/sent email related data over the access network 1610, web browsing service billing for data usage associated with received/sent web browsing related data over the access network 1610 and/or any other network based service, and/or any transactional based services, such as for multimedia content purchases or other transactions).

[0232] In some embodiments, verifiable device based service billing is provided by sending dummy(/test) billing events, such as having an access control integrity server 1654 of the service controller 122 instruct the access control integrity agent 1694 to send a dummy(/test) billing event to the billing agent 1695. If the billing agent does not then send the expected report, which should reflect the dummy(/test) (or fails to timely send any report), then the system can verify whether the billing process is working properly. In addition, a dummy (/test) transaction can be used to verify transaction based billing through a variety of approaches (e.g., the access control integrity agent 1694 can similarly send a dummy(/test) transactional billing event to the billing agent 1695 as a test to determine whether the billing agent 1695 then provides the expected report reflecting that dummy(/test) transaction). For example, the test billing events can be trapped by a device assisted billing mediation server and removed from the user account billing.

[0233] In some embodiments, verifiable device based service billing is provided by sending one or more data bursts to the device to confirm that data was received and to confirm that the service monitor agent 1696 properly logged the data burst(s) in the local service usage or

service activity counter. In some embodiments, data bursts can be used to verify data throttling (e.g., if the device has exceeded service data usage limits and/or is approaching such limits such that service data usage should be throttled, then sending data bursts can be used to verify whether the expected throttling is properly being performed on the device). In some embodiments, verifiable device based service billing is provided by submitting requests to connect to an unauthorized service/website to verify if that unauthorized service usage is properly blocked. In some embodiments, verifiable device based service billing is provided by submitting requests to perform an unauthorized transaction to verify if that unauthorized transaction is properly blocked.

[0234] In some embodiments, verifiable device based service billing is provided by verifying device service activities relative to IPDRs for the device. In some embodiments, the IPDRs for the device (possibly in a modified format) are periodically and/or upon request sent to the device, as described herein. For example, IPDRs for the device can be compared to the device's local service data usage counter and/or to the service plan for the device to determine if the overall service data usage limit has been exceeded, whether out of plan/unauthorized/unrecorded websites/other services have been performed by the device, whether service plan/profile bandwidth limits have been exceeded, whether out of plan/unauthorized/unrecorded transactions have been performed (e.g., verifying IPDR transaction logs, assuming such are included in the IPDRs, with the local transaction logs of the device to determine, for example, whether the local device records indicate that fewer than the network recorded number of content downloads, such as downloaded songs, were purchased), and/or whether any other activities verifiable based on a comparison of IPDRs indicate that the device has been used in any manner that is out of or exceeds the service plan/profile for the device.

[0235] In some embodiments, device based service billing includes recording billing option response history. For example, this approach can be particularly important for service plan overage conditions (e.g., when the use of the device is exceeding the service plan associated with the device in some manner, such as service data usage, bandwidth, service or transaction access and/or in some other manner). In some embodiments, in a service plan overage condition, the user is requested to confirm that user has acknowledged notification of service plan overage,

such as via the user interface 1697. In some embodiments, such service plan overage acknowledgements require that the user enter a unique identification to validate authorization by the user identity associated with the device (e.g., another type of verification mechanism, in the event a device is stolen or being used by someone other than the authorized user of the device, then that unauthorized user would not be able to confirm the service plan overage acknowledgement, and appropriate actions can then be taken, such as throttling, quarantining or (temporarily) suspending service/network access). In some embodiments, if the device is compromised/hacked (e.g., by the user of the device), and the device is used in a manner that results in a service usage overage (e.g., determined based on device assisted service usage monitoring, and/or network based service usage monitoring using IPDRs/CDRs), then the billing system determines billing for such service usage overage costs. This overage billing can be initiated by the device 100 (e.g., service processor 115), the service controller 122, the billing system 123, the AAA 121, or some other network function. In some embodiments, if the device is compromised/hacked (e.g., by a user of the device), and the device is used in a manner that results in a service usage overage, one or more of the following actions is taken: the user is notified, the user is required to acknowledge the notification, the device traffic is sent to SPAN (or similar traffic sampling and analysis function), and/or the device is flagged for further analysis.

[0236] In some embodiments, device based service billing includes an option to bill by account, such as to bill different service activities and/or transactions to a specified account (e.g., other than the user's account associated with the general service plan for the device). For example, bill by account can provide for billing according to application, content type, website, transaction, network chatter (e.g., heartbeat communications and/or other network traffic that is used by, for example, the central/service provider to generally maintain network access for the device), and/or transaction partner sponsored activities and then report such bill by account information for billing mediation/reconciliation. For example, a bill by account report can be sent by billing agent 1695 from the device to central billing 1619 (e.g., as a billing event); or alternatively, sent to an intermediate server/aggregator, which can then reformat and send the reformatted report to central billing 1619 (e.g., providing the billing report in a format required by central billing 1619); or alternatively, sent to a mediation server, which can re-compute the billing based on the bill by account report (e.g., offset the bill based on network chatter,

transaction based billing, transaction partner sponsored activities, content providers, website providers and/or advertising providers) and then send the recomputed (and potentially reformatted) report to central billing 1619.

[0237] In some embodiments, one or more of the mediation/reconciliation functions for device assisted billing, device generated billing events, device generated bill by account events and device generated open transaction billing events can be implemented in the service controller 122 (e.g., the billing event server 1662) or in another function located in the billing system 123 or elsewhere. This billing mediation server function accepts the device based billing events discussed immediately above, reformats the billing events into a format accepted and recognized by the billing system, mediates the billing event information to remove service usage billing from the user account and place it in other bill by account categories as appropriate according to the bill by account mediation rules, adds other billing events for service usage or transactions to the user account as appropriate according to the device based billing rules, and then applies the information to the billing information the user account to correct or update the account.

[0238] For example, a bill by account can allow for a website provider, such as Google or Yahoo, to pay for or offset certain account usage for web browsing, web based searching, web based email, or any other web based or other service usage activities, which may also be based (in whole or in part) on the activities performed by the user on such transactional services (e.g., based on advertisement viewing/accessing or click-through activities by the user, by which an advertisement business model used by such website providers directly or indirectly supports such service account subsidies). As another example, a bill by account can allow for an advertiser to pay for or offset certain account usage for viewing and/or accessing (e.g., clicking through) a web placed advertisement or other advertisement sent via the network to the device. As yet another example, various network chatter (e.g., heartbeat related network and other network chatter related service data usage) can be assigned to a dummy account and such can be used to offset the bill and/or used for tracking the data usage for such activities for the device. In another example, service data usage for access to a transactional service, such as a multimedia content download service (e.g., music, eBook, music/video streaming, and/or movie or other multimedia content download service), or an online shopping site (e.g., Amazon, eBay or another online shopping site), can be billed to a transactional service account assigned to a transactional

service partner that sponsors access to that sponsor's transactional service, thereby allowing that transactional service partner to pay for or offset (e.g., subsidize) the account usage for such activities, which may also be based (in whole or in part) on the transactions actually performed by the user on such transactional services (e.g., based on the volume/cost of the multimedia service download purchases by the user and/or online activities).

[0239] In some embodiments, device based service billing includes recording billing events on the device and then reporting such billing to the network (e.g., central billing 1619). In some embodiments, device based service billing includes reporting service usage events and/or applying cost look-up and logging/reporting service billing updates. For example, this allows for reporting not only service usage but also cost of such service usage to the user via the user interface of device 100. Also, for example, the cost of such service usage can also be reported to the billing server. In some embodiments, device based service billing includes reporting service usage to the network, and the network determines the cost for such service usage.

[0240] In some embodiments, billing information for roaming partners is provided. For example, a roaming server can include a roaming service cost data table for roaming service partners. In this example, when the device (e.g., device 100) connects to a roaming network provided by a roaming service partner, then the device can also receive the roaming service data rate based on the roaming service cost data table provided by the roaming server. Alternatively, the roaming server can send the roaming service cost data table (or a modified format of the same) to the device thereby allowing the device to determine the costs for such roaming network service usage or service activity. As described herein, the device can also automatically use a roaming service profile when connecting to the roaming network service and/or the user can be notified of the roaming service profile options based on the roaming service data costs and then select the desired roaming service profile accordingly.

[0241] In some embodiments, the user is provided with a list of service costs based on locally stored roaming table and a search of available roaming partners that the device 100 detects and can connect to. In some embodiments, the user is provided with a projected cost per day for one or more roaming service provider options based on typical service usage history and the cost for each service provider. In some embodiments, the user is provided with a set of

options for service usage notification, controlling or throttling service usage and/or cost while roaming (e.g., using the service notification and cost control techniques as similarly discussed herein but applied to the roaming network). In some embodiments, these controls are set by a VSP (or, e.g., an IT manager using VSP functions). In some embodiments, roaming tables are updated periodically in the background while on a home network (or other low cost network) and cached. In some embodiments, cache updates occur based on fixed time period (e.g., late at night when updates are less expensive due to network inactivity). In some embodiments, the roaming partner cost table cache updates are done whenever connected to a desirable network that is not as expensive or bandwidth constrained (e.g., at home, work, or off the WWAN). In some embodiments, updates occur at time of day that network is not busy. In some embodiments, updates occur based on network push when roaming table is changed (e.g., one or more of the roaming partners changes the rate). In some embodiments, the service cost to update the roaming service cost table is charged to bill by account and possibly not charged to end user. In some embodiments, the roaming service center is provided as a service that is paid for (e.g., potentially bill by account tracks all related costs). For example, this type of roaming cost control can be provided as a service through central provider, MVNO, roaming partner provider, VSP or as a third party application not associated with any service provider (e.g., IT manager). For example, the controls for how to update cache, set service control policies, and other controls can be defined by any number of VSP entities including the user through a website service.

[0242] In some embodiments, a roaming service center is provided as a service in which, for example, the user is provided with a list of service costs based on a locally stored (or remotely accessed) roaming table. In some embodiments, the roaming service center provides the user with a projected cost per day for one or more roaming service provider options based on typical service usage history and the cost for each service provider. In some embodiments, the roaming service center provides the user with a set of options for controlling/throttling usage and/or cost while roaming. In some embodiments, these controls are set by a VSP (e.g., an IT manager using VSP functions). For example, roaming tables can be updated periodically in the background while on a home network and cached. In some embodiments, cache updates occur based on a fixed time period. In some embodiments, the roaming partner cost table cache updates are done whenever the device is connected to a desirable network that is not as

expensive or bandwidth constrained (e.g., at home, work and/or off the WWAN). In some embodiments, updates occur at time of day that network is not busy. In some embodiments, updates occur based on a network push when a roaming table is changed (e.g., one or more of the roaming partners changes the rate). In some embodiments, the service cost to update the roaming service cost table is charged to bill by account and possibly not charged to the user. In some embodiments, the roaming service center is provided as a service that is paid for by the user and/or part of a service plan. In some embodiments, a bill by account function tracks all related costs. For example, the roaming service center can be provided as a service through central provider, MVNO, roaming partner provider, VSP or as a third party application not associated with any service provider (e.g., IT manager).

[0243] In some embodiments, a synchronized local service usage counter based on time stamped central billing information is provided. For example, the local service usage counter, as similarly described above, can also be synchronized to past service usage records (e.g., time stamped central billing records of service usage for the device) and use local estimates for current/present service usage estimates for the device. In this example, the central billing system (e.g., central billing 1619) can push the time stamped central billing information to the device (e.g., device 100), the device can pull the time stamped central billing information, and/or an intermediate server can provide a mediated push or pull process. In some embodiments, synchronization is performing periodically based on service usage levels with free-running estimates between synchronizations.

[0244] In some embodiments, service usage is projected based on calculated estimates of service usage based on synchronized service usage and local service usage count information. For example, projected service usage can be calculated on the device or calculated on a server (e.g., a billing server or an intermediate billing server), which provides the calculated projected service usage information to the device, such as using various adaptive algorithms for service usage projections. For example, an adaptive algorithm can use historical/past synchronized network service usage information (e.g., synchronized with local service usage data based on time stamps associated with IPDRs) to assist in service usage projections, based on, for example, total service usage count, service usage count by certain service related criteria (e.g., application, content, service type, website and/or time of day). In another example, an adaptive algorithm

synchronizes to past service usage data (e.g., the local estimate of past service usage data is updated to be synchronized up through the point in time associated with the latest IPDR time stamp that has been received) and current local estimates of service usage collected since the latest time stamp are then added to the time stamped IPDR service usage counter to minimize the service usage counter offset so that it is no greater than the difference between the network service usage measure and the local service usage measure since the latest IPDR time stamp. In some embodiments, these adaptive algorithm techniques are performed on the device and/or performed on the network (e.g., on a network server) for processing. In some embodiments, if there is an offset in the local device based service usage count between IPDR synchronization events and the IPDR service usage count between IPDR synchronization events, then an algorithm can be employed to estimate any systematic sources for the offset and correct the local service usage count to minimize the offsets. As an example, if the IPDR service usage count is typically off by a fixed percentage, either high or low, then an algorithm can be employed to estimate a multiplier that is applied to the local service usage count to minimize the offset between IPDR service usage synchronization events. In another example, there can be a consistent constant offset and a multiplier offset, both of which can be estimated and corrected for. Those of ordinary skill in the art will appreciate that more sophisticated algorithms can be employed to estimate the nature of any systematic offsets, including, for example, offsets that occur due to specific service usage activities or network chatter to manage the device, and such offsets can then be minimized between IPDR service synchronization events. In some embodiments, synchronized service usage data is used to create an improved analysis of the statistical patterns of service usage to provide more accurate service usage projections. Those of ordinary skill in the art will also appreciate that a variety of additional adaptive algorithm techniques can be used including those that provide for various statistical analysis techniques and/or other techniques.

[0245] In some embodiments, service usage is projected for the end of a billing/service period for a service plan versus the service usage allowed under the service plan for that billing/service period. A display of excess charges is also provided for the projected rate of service usage based on the monitored service usage behavior through the end of the billing/service period (e.g., this can be zero if the service usage is projected to be less than that allowed under the service plan and a positive cost number if it is projected to be more than the

service plan). For example, this can be implemented in numerous ways, such as on a server in the network, on a gateway/router/switch in the network, and/or on the device, as discussed below and generally described herein with respect to other service/cost usage monitoring and notification embodiments. If implemented in the network server or gateway/router/switch, then the service/cost usage projections and related information can be pushed to the device, or the device can be notified that such information is available to pull and/or periodically pushed/pulled. The service usage information/estimates can be collected from the device, the network or both (e.g., reconciled and/or synchronized) as similarly described herein. The service usage information/estimates are then analyzed to determine service usage/cost projects as similarly described herein and compared to the service plan for the device to determine the projected service/cost usage overage (if any). In some embodiments, one or more of the following are determined by, reported to and/or displayed on the device: service usage value, projected service usage value, service usage plan limit, projected service usage overage, projected service cost overage, service plan period time duration, service plan time remaining before end of period and/or other pertinent information.

[0246] In some embodiments, the device also determines service costs based on the synchronized service usage count thereby allowing the device to also report the service cost information to the user. For example, the device can locally store a service cost look-up table(s), locally store different service cost look-up tables for different networks and/or for roaming networks, and/or request such information from a billing or intermediate billing server (and/or a roaming server) on the network. As another example, the device can obtain the calculated service costs based on the synchronized local service usage count and/or network service usage count from an intermediate server (e.g., a billing or intermediate billing server) thereby offloading the computational costs associated with calculated these projections and the data storage for service cost lookup tables onto the intermediate server on the network using the network service usage counter with or, alternatively, without the synchronized local service usage counter.

[0247] In some embodiments, service usage count categorization by network (e.g., a home network (such as a Wi-Fi, WAN, femtocell or other home network) versus a roaming network) is provided. Similarly, the synchronized local service usage counter can be

synchronized by network. Also, a synchronized local service usage count for networks controlled by a central provider, for networks controlled by other providers (e.g., MVNO), and/or free networks can similarly be provided.

[0248] In some embodiments, a service notification and billing interface is provided. For example, service usage and projected service usage, such as described herein, can be displayed to the user of the device (e.g., via user interface 1697). Similarly, expected/projected service or cost overrun/overage, such as described herein, can also be displayed to the user. As another example, a most cost effective plan can be determined/projected based on historical and/or projected service usage, and this determined/projected most cost effective plan can be displayed to the user. In yet another example, a list of available networks accessible by the device can be displayed to the user. In this example, one or more undesired available networks can also be blocked from display thereby only displaying to the user desired and/or preferred available networks. In this example, service usage plans and/or service usage plan option comparison for one or more alternative networks or roaming networks can also be displayed to the user. Similarly, service cost plans and/or service/cost plan option comparison for one or more alternative networks or roaming networks can also be displayed to the user. In addition, roaming service usage, projected roaming service usage, estimated roaming service cost, and/or projected estimated roaming service cost can also be displayed to the user. These roaming service usage/costs can also be displayed to the user so that the user can utilize this information for selecting various roaming service billing options. In another example, alternative and/or least cost networks are determined and displayed to the user. In another example, alternative warnings are displayed to the user for any or specified roaming networks.

[0249] In some embodiments, the service notification and billing interface notifies the user of expected network coverage (e.g., based on the device's current geography/location and the accessible networks for the device from that current geography/location) and displays options to the user based on the expected network coverage information. In some embodiments, the service notification and billing interface notifies the user of their current service usage at specified service usage points and displays various options to the user (e.g., service usage options and/or billing options). For example, the user's responses to the presented options are recorded (e.g., stored locally on the device at least temporarily for reporting purposes or

permanently in a local configuration data store until such configuration settings are otherwise modified or reset) and reported, such as to the billing server (e.g., central billing 1619). For example, user input, such as selected options and/or corresponding policy settings, can be stored locally on the device via a cache system. As another example, the service notification and billing interface displays options to the user for how the user wants to be notified and how the user wants to control service usage costs, the user's input on such notification options is recorded, and the cost control options (e.g., and the billing agent 1695 and policy control agent 1692) are configured accordingly. Similarly, the user's input on service plan options/changes can be recorded, and the service plan options/changes (e.g., and the billing agent 1695 and policy control agent 1692) are configured/updated accordingly. In another example, the service notification and billing interface provides various traffic control profiles, such as for where the user requests assistance in controlling service usage costs (e.g., service data usage and/or transactional usage related activities/costs). Similarly, the service notification and billing interface can provide various notification options, such as for where the user wants advance warning on service coverage. In another example, the service notification and billing interface provides options for automatic pre-buy at a set point in service usage. In another example, the service notification and billing interface provides the option to choose different notification and cost control options for alternative networks or roaming networks.

[0250] In some embodiments, an online portal or web server is provided for allowing the user to select and/or update policy settings. For example, user input provided via the online portal/web server can be recorded and reported to the billing server (e.g., central billing 1619). In another example, the online portal/web server can display transaction billing information and/or accept input for a transaction billing request, which can then be reported to the billing server accordingly.

[0251] As shown in FIG. 16, the service processor 115 includes a service interface or user interface 1697. In some embodiments, the user interface 1697 provides the user with information and accepts user choices or preferences on one or more of the following: user service information, user billing information, service activation, service plan selection or change, service usage or service activity counters, remaining service status, service usage projections, service usage overage possibility warnings, service cost status, service cost projections, service

usage control policy options, privacy/CRM/GPS related options, and/or other service related information, settings, and/or options. For example, the user interface 1697 can collect service usage information from service monitor agent 1696 to update the local service usage counter (and/or, alternatively, the service usage information is obtained from the service controller 122) to update user interface service usage or service cost information for display to the user. As another example, service billing records obtained from central billing system 1619 can be used to synchronize local service usage counters and service monitor agent 1696 information to perform real-time updating of local service usage counters between billing system 1619 synchronizations. As another example, the user interface 1697 can display options and accept user preference feedback, such as similarly discussed above with respect to user privacy/CRM/GPS filtering, traffic monitoring and service controls. For example, the user interface 1697 can allow the user of the device to modify their privacy settings, provide user feedback on service preferences and/or service experiences, modify their service profiles (e.g., preferences, settings, configurations, and/or network settings and options), to review service usage data (e.g., based on local service usage counters and/or other data monitored by the service processor 115), to receive various events or triggers (e.g., based on projected service usage/costs), and/or the user interface 1697 can provide/support various other user input/output for service control and service usage.

[0252] In some embodiments, by providing the service policy implementation and the control of service policy implementation to the preferences of the user, and/or by providing the user with the option of specifying or influencing how the various service notification and control policies or control algorithms are implemented, the user is provided with options for how to control the service experience, the service cost, the capabilities of the service, the manner in which the user is notified regarding service usage or service cost, the level of sensitive user information that is shared with the network or service provider entity, and the manner in which certain service usage activities may or may not be throttled, accelerated, blocked, enabled and/or otherwise controlled. Accordingly, some embodiments provide the service control to beneficially optimize user cost versus service capabilities or capacities in a manner that facilitates an optimized user experience and does not violate network neutrality goals, regulations and/or requirements. For example, by offering the user with a set of choices, ranging from simple choices between two or more pre-packaged service control settings options to advanced user screens where more detailed level of user specification and control is made

available, some embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, and/or other “entity” to implement valuable or necessary service controls while allowing the user to decide or influence the decision on which service usage activities are controlled, such as how they are controlled or throttled and which service usage activities may not be throttled or controlled in some manner. These various embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, or other “entity” to assist the user in managing services in a manner that is network neutral with respect to their implementation and service control policies, because the user is making or influencing the decisions, for example, on cost versus service capabilities or quality. By further providing user control or influence on the filtering settings for the service usage reporting or CRM reporting, various levels of service usage and other user information associated with device usage can be transmitted to the network, service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, and/or other “entity” in a manner specified or influenced by the user to maintain the user’s desired level of information privacy.

[0253] As shown in FIG. 16, the service processor 115 includes the service downloader 1663. In some embodiments, the service downloader 1663 provides a download function to install or update service software elements on the device. In some embodiments, the service downloader 1663 requires a secure signed version of software before a download is accepted. For example, the download can require a unique key for a particular service downloader 1663. As another example, the service downloader 1663 can be stored or execute in secure memory or execute a secure memory partition in the CPU memory space. Those of ordinary skill in the art will appreciate that there are a variety of other security techniques that can be used to ensure the integrity of the service downloader 1663.

[0254] As shown in FIG. 16, the service processor 115 includes a modem driver 1640. In some embodiments, the modem driver 1640 converts data traffic into modem bus (not shown) traffic for one or more modems via the modem firewall 1655. As shown in FIG. 18, in some embodiments, modem selection and control 1811 selects the access network connection and is in communication with the modem firewall 1655, and modem drivers 1831, 1815, 1814, 1813, 1812 convert data traffic into modem bus traffic for one or more modems and are in

communication with the modem selection and control 1811. As shown in FIG. 21, in some embodiments, modems 2141, 2125, 2124, 2123, 2122, which are in communication with the modem bus 2120, connect the device to one or more networks. In some embodiments, different profiles are selected based on the selected network connection (e.g., different service profiles/policies for WWAN, WLAN, WPAN, Ethernet and/or DSL network connections), which is also referred to herein as multimode profile setting. For example, service profile settings can be based on the actual access network (e.g., home DSL/cable or work network) behind the Wi-Fi not the fact that it is Wi-Fi (or any other network, such as DSL/cable, satellite, or T-1), which is viewed as different than accessing a Wi-Fi network at the coffee shop. For example, in a Wi-Fi hotspot situation in which there are a significant number of users on a DSL or T-1 backhaul, the service controller can sit in a service provider cloud or an MVNO cloud, the service controls can be provided by a VSP capability offered by the service provider (e.g., as described herein with respect to FIG. 49) or the service controller can be owned by the hotspot service provider that uses the service controller on their own without any association with an access network service provider. For example, the service processors can be controlled by the service controller to divide up the available bandwidth at the hotspot according to QoS or user sharing rules (e.g., with some users having higher differentiated priority (potentially for higher service payments) than other users). As another example, ambient services (as similarly described herein) can be provided for the hotspot for verified service processors.

[0255] In some embodiments, the service processor 115 and service controller 122 are capable of assigning multiple service profiles associated with multiple service plans that the user chooses individually or in combination as a package. For example, a device 100 starts with ambient services that include free transaction services wherein the user pays for transactions or events rather than the basic service (e.g., a news service, eReader, PND service, pay as you go session Internet) in which each service is supported with a bill by account capability to correctly account for any subsidized partner billing to provide the transaction services (e.g., Barnes and Noble may pay for the eReader service and offer a revenue share to the service provider for any book or magazine transactions purchased from the device 100). In some embodiments, the bill by account service can also track the transactions and, in some embodiments, advertisements for the purpose of revenue sharing, all using the service monitoring capabilities disclosed herein. After initiating services with the free ambient service discussed above, the user may later choose

a post-pay monthly Internet, email and SMS service. In this case, the service controller 122 would obtain from the billing system 123 in the case of network based billing (or in some embodiments the service controller 122 billing event server 1622 in the case of device based billing) the billing plan code for the new Internet, email and SMS service. In some embodiments, this code is cross referenced in a database (e.g., the policy management server 1652) to find the appropriate service profile for the new service in combination with the initial ambient service. The new superset service profile is then applied so that the user maintains free access to the ambient services, and the billing partners continue to subsidize those services, the user also gets access to Internet services and may choose the service control profile (e.g., from one of the embodiments disclosed herein). The superset profile is the profile that provides the combined capabilities of two or more service profiles when the profiles are applied to the same device 100 service processor. In some embodiments, the device 100 (service processor 115) can determine the superset profile rather than the service controller 122 when more than one “stackable” service is selected by the user or otherwise applied to the device. The flexibility of the service processor 115 and service controller 122 embodiments described herein allow for a large variety of service profiles to be defined and applied individually or as a superset to achieve the desired device 100 service features.

[0256] As shown in FIG. 16, the service controller 122 includes a service control server link 1638. In some embodiments, device based service control techniques involving supervision across a network (e.g., on the control plane) are more sophisticated, and for such it is increasingly important to have an efficient and flexible control plane communication link between the device agents (e.g., of the service processor 115) and the network elements (e.g., of the service controller 122) communicating with, controlling, monitoring, or verifying service policy. For example, the communication link between the service control server link 1638 of service controller 122 and the service control device link 1691 of the service processor 115 can provide an efficient and flexible control plane communication link, a service control link 1653 as shown in FIG. 16, and, in some embodiments, this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor 115 and the service controller 122. In some embodiments, the service control server link 1638 provides the network side of a system for transmission and reception of service agent to/from network element functions. In some

embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions (e.g., thereby reducing network chatter). In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency and/or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security and/or encryption are used to secure the link against potential discovery, eavesdropping or compromise of communications on the link. In some embodiments, the service control server link 1638 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments described herein for the service control server link 1638 provide an efficient and secure mechanism for transmitting and receiving service policy implementation, control, monitoring and verification information between the device agents (e.g., service processor agents/components) and other network elements (e.g., service controller agents/components).

[0257] In some embodiments, the service control server link 1638 can employ the counterpart service control plane secure transmission methods discussed above with respect to the service control device link 1691. For example, one or more layers of security can be used to secure the communications link, including, for example, basic IP layer security, TCP layer security, service control link layer security, and/or security specific from service controller servers to service processor agents.

[0258] In some embodiments, the service control server link 1638 reduces network chatter by efficiently transmitting service control related communications over the link. For example, the service control server link 1638 can transmit server messages asynchronously as they arrive. As another example, the service control server link 1638 can perform collection or buffering of server messages between transmissions. As another example, the service control server link 1638 can determine when to transmit based potentially on several parameters, such as one or more of: periodic timer trigger, waiting until a certain amount of service usage or traffic usage has occurred, responding to a service agent message, responding to a service agent request, initiated by one or more servers, initiated by a verification error condition, and/or initiated by some other error condition. For example, once a transmission trigger has occurred, the service control server link 1638 can take all buffered agent communications and frame the communications. In addition, the service control server link 1638 can provide for an efficient

communication link based on various embodiments related to the timing of transmissions over the service control link, as similarly discussed above with respect to the service control device link 1691 description. For example, the timing functions, such as asynchronous messages or polling for messages, constant frequency transmission, transmission based on how much service usage or data traffic usage has taken place, transmission in response to device side control link message, service verification error events, other error events, and/or other message transmission trigger criteria can be determined, controlled and/or initiated by either the device side or the network side depending on the embodiment.

[0259] In some embodiments, the service control server link 1638 provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link 1653. For example, the service control server link 1638 can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link 1638 further secures the communications with transport layer encryption, such as TCP TLS or another secure transport layer protocol. As another example, the service control server link 1638 can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

[0260] In some embodiments, the service control server link 1638 includes the agent heartbeat function in which the agents provide certain required reports to the service processor for the purpose of service policy implementation verification or for other purposes. For example, the heartbeat function can also be used to issue queries or challenges, messages, service settings, service control objectives, information requests or polling, error checks and/or other communications to the agents. As another example, agent heartbeat messages can be in the open or encrypted, signed and/or otherwise secured. Additional heartbeat function and the content of heartbeat messages can be provided as similarly described herein, such as described above with respect to the service control device link 1691 and the access control integrity agent 1694 and other sections. In some embodiments, the service controller 122 and/or agents of the service controller 122 are programmed to periodically provide reports, such as upon a heartbeat response (e.g., an agent can repeatedly send necessary reports each heartbeat), and appropriate actions can then be taken based upon such received reports. Accordingly, the heartbeat function

provides an important and efficient system in various embodiments described herein for verifying the service policy implementation and/or protecting against compromise events. There are many other functions the agent heartbeat service can perform many of which are discussed herein, while many others will be apparent to one of ordinary skill in the art given the principles, design background and various embodiments provided herein.

[0261] In some embodiments, the service control server link 1638 also provides a service control software download function for various embodiments, which, for example, can include a download of new service software elements, revisions of service software elements, and/or dynamic refreshes of service software elements of the service processor 115 on the device. In some embodiments, this function is performed by the service control server link 1638 transmitting the service control software as a single file over the service control link. For example, the file can have encryption or signed encryption beyond any provided by the communication link protocol itself for service control link 1653. In another example, the service control software files can be segmented/divided into smaller packets that are transmitted in multiple messages sent over the service control link 1653. In yet another example, the service control software files can be transmitted using other delivery mechanism, such as a direct TCP socket connection from a service download control server 1660, which can also involve secure transport and additional levels of encryption. In some embodiments, the service control server link 1638 and/or service download control server 1660 use(s) an agent serial number and/or a security key look up when agents are updated and/or when a dynamic agent download occurs.

[0262] As shown in FIG. 16, the service controller 122 includes an access control integrity server 1654. In some embodiments, the access control integrity server 1654 collects device information on service policy, service usage, agent configuration and/or agent behavior. For example, the access control integrity server 1654 can cross check this information to identify integrity breaches in the service policy implementation and control system. In another example, the access control integrity server 1654 can initiate action when a service policy violation or a system integrity breach is suspected.

[0263] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) acts on access control integrity agent reports and error

conditions. Many of the access control integrity agent 1654 checks can be accomplished by the server. For example, the access control integrity agent 1654 checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

[0264] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy implementations by comparing various service usage measures (e.g., based on network monitored information, such as by using IPDRs, and/or local service usage monitoring information) against expected service usage behavior given the policies that are intended to be in place. For example, device service policy implementations can include measuring total data passed, data passed in a period of time, IP addresses, data per IP address, and/or other measures such as location, downloads, email accessed, URLs, and comparing such measures expected service usage behavior given the policies that are intended to be in place.

[0265] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy, and the verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: unauthorized network access (e.g., access beyond ambient service policy limits); unauthorized network speed (e.g., average speed beyond service policy limit); network data amount does not match policy limit (e.g., device not stop at limit without re-up/revising service policy); unauthorized network address; unauthorized service usage (e.g., VOIP, email, and/or web browsing); unauthorized application usage (e.g., email, VOIP, email, and/or web); service usage rate too high for plan, and policy controller not controlling/throttling it down; and/or any other mismatch in service measure and service policy.

[0266] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy based at least in part on, for example, various error conditions that indicate a mismatch in service measure and service policy. For example, various verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: mismatch in one service

measure and another service measure; agent failure to report in; agent failure to respond to queries (e.g., challenge-response sequence and/or expected periodic agent reporting); agent failure to respond correctly to challenge/response sequence; agent improperly configured; agent failure in self checks; agent failure in cross-checks; unauthorized agent communication or attempted unauthorized communication; failure in service policy implementation test; failure in service usage reporting test; failure in service usage billing test; failure in transaction billing test; failure in download sequence; environment compromise event, such as unauthorized software load or execution (or attempt), unauthorized memory access (or attempt), unauthorized agent access (or attempt), known harmful software, and/or known harmful communications signature; and/or failure to respond to various messages, such as send message and suspend and/or send message and quarantine. In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy by performing automated queries and analysis, which are then reported (e.g., anomalous/suspicious report results can be reported for further analysis by a person responsible for determining whether such activities indicate out of policy activities or to provide information to the user to inform the user of such anomalous/suspicious report results that may indicate out of policy activities). For example, the user can review the report to authorize whether such activities were performed by the user (e.g., website access requests, specific transactions, and/or phone calls) and/or indicate that such activities were not authorized by the user (e.g., indicate a potential compromise of the device, such as by malware or other unauthorized software/user use of the device). In another example, the user can also be connected to communicate with service support of the service provider regarding such reported activities (e.g., by text/chat, voice/phone, and/or video conference to a service support). Accordingly, in some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) provides a policy/service control integrity service to continually (e.g., periodically and/or based on trigger events) verify that the service control of the device has not been compromised and/or is not behaving out of policy.

[0267] In some embodiments, upon detection of one or more service verification errors, such as the various service verification errors discussed above, the device is directed to a quarantine network status in which the device can, for example, only access network control plane functions, billing functions, and other functions generally controlled by the access network

service provider or the central service provider. For example, quarantine network access restrictions and routing can be accomplished with the access network AAA and routing system (e.g., access network AAA server 1621 and one or more of the gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720) or can be accomplished with device based access control or traffic control policy implementation. Quarantine network equipment or servers can, for example, be located within the access network or within another network with access to the access network. Communication with the quarantine network infrastructure can be accomplished, for example, with a secure link with one or more encryption levels or a dedicated private link. In some embodiments, quarantining a device includes, for example, a two step process for routing quarantine network device traffic, first, to a quarantine traffic handling router or server and, second, from there to the actual quarantine network infrastructure, with the route being determined by device parameters, user parameters, access service provider parameters or other parameters associated with the quarantine network routing. In some embodiments, the device is completely suspended from the network in which, for example, the device can first issue a user interface message to the user or issuing another form of a message to the user or service subscriber, such as via email, hard copy message and/or voice message. In some embodiments, the device network access, service capabilities and/or traffic shaping are limited, partially restricted or completely restricted, service capabilities. For example, these limitations and/or restrictions can be implemented in the device and/or in the network. For example, implementing a device quarantine (e.g., using a RADIUS server to quarantine the device) can involve assigning the device to a different billing profile.

[0268] In some embodiments, upon detection of one or more service verification errors, such as the various service verification errors discussed above, switch based port analysis is performed to further monitor the device (e.g., referred to as Switched Port Analyzer (SPAN) on Cisco switches, and various other vendors have different names for it, such as Roving Analysis Port (RAP) on 3Com switches). In some embodiments, the device service policy implementation behavior is monitored at a deeper level in the network by copying device traffic in the switch so that it goes to both an intended data path destination and to a specified port for switch based port analysis (e.g., the traffic content can be analyzed and recorded using deep packet inspection (DPI) techniques, which can provide a finer level of detail than the typical IPDR). For example, an advantage of performing a switch based port analysis function is that

the traffic need not be analyzed in real time, and a sample subset of the devices on the network can be selected for such analysis based on, for example, either identifying devices that have suspect service policy implementation behavior and/or a regular sampling algorithm that eventually samples all devices, or some other selection approaches. As another example, a scheduled switch based port analysis sampling can be applied that eventually rotates through all devices and designates a higher priority in the sampling queue for devices that are suspect.

[0269] In some embodiments, switch based port analysis allows for off-line sampled or non-real-time DPI, as described above, as a verification measure for the device based service control measures that are implemented. In some embodiments, sophisticated DPI techniques are used to enhance the content of the IPDRs so that they provide detailed information that can be made available in the network. For example, some of the DPI packet analysis may be redundant between the device and the network, but this approach provides for a much finer grain validation for the device based service and less reliance on the device for some of the service traffic analysis that service providers need. In some embodiments, the device control server functions and the service control policy verification functions are implemented in an integrated hardware/software system (e.g., a gateway, server, router, switch, base station, base station aggregator, AAA server cluster or any other hardware or hardware/software system) located in the network that the network level traffic inspection is accomplished in, or in one or more servers integrated to operate in a coordinated manner with the DPI boxes. In some embodiments, the device control server functions and the service control policy verification functions are implemented in an integrated hardware/software system (e.g., a gateway, server, router, switch, base station, base station aggregator, AAA server cluster or any other hardware or hardware/software system) located in the network that provides deep service control capability (e.g., using DPI techniques) for devices that have some or all of the service processor functions installed and, in some embodiments, also providing coarser network control of the basics for devices that do not have a service processor installed in the device (e.g., such coarser network control functions include max data rate and/or max total data).

[0270] In some embodiments, the SPAN function is used in a revolving periodic manner as well to augment CDR data with deeper packet information for the purpose of spot-checking device based service usage measures. Examples of where this can be beneficial include spot

checking network address access policies, spot checking ambient access policies, spot checking billing event reports, spot checking intermediate networking device/end point device count (via checking network source or destination addresses, token, cookies or other credentials, etc). For example, the periodic SPAN can be scheduled for all devices equally, for certain devices or users with higher priority, frequency or depth of SPAN than others, higher priority, higher frequency or immediate priority for devices with higher usage patterns or unusual usage patterns, immediate or very high priority for devices with a policy violation status.

[0271] In some embodiments, a combination traffic inspection and service control approach implements traffic and service control functions in the network that are conducive for a network based implementation and implements traffic and service control functions in the device that are either more conducive for performing in the device or can only be performed in the device (e.g., activities involving inspection of traffic that is encrypted once it is transmitted to the network). For example, using this approach, activities that can be done in the network are generally performed in the network and/or are more efficiently performed in the network than the device, and activities that are more efficiently performed in the device or can only be performed in the device are performed in the device (e.g., depending on device processing/storage capabilities and/or other design/security considerations). For example, the following are various traffic and service control functions that, in some embodiments, are preferably or can only be performed in the device: network based packet processing capability limitations (e.g., encrypted traffic, application layer information unavailable once the traffic goes into the networking stack, other application/usage context information available on the device but not in the network); information that is generally/preferably maintained and processed locally in the device for network neutrality reasons (e.g., network neutrality issues can generally be efficiently implemented by keeping all, substantially all or at least some aspect of decisions on how to implement algorithms to control traffic local to the device and under user decision control, and/or by providing the user with a set of pre-packaged choices on how to manage service usage or service activity usage or manage service usage versus service cost or price); information that is generally/preferably maintained and processed locally in the device for user privacy reasons (e.g., deeper levels of traffic monitoring and service usage monitoring data where it is available for assisting the user in achieving the best, lowest cost experience and implementing a CRM filter function to the user so that the user can control the level of CRM the network is allowed to

receive, such as with the higher levels of information being exchanged for something of value to the user, and/or user location information); information that is generally/preferably maintained and processed locally in the device for the purpose of informing the user of service control settings or service activity usage or to adjust service activity control settings or receive user feedback to choices regarding service usage policies or billing options (e.g., providing the user with a UI for the purpose of monitoring an estimate of service usage and/or notifying the user of at least some aspect of estimated service usage or projected service usage, providing the user with a UI for the purpose of monitoring an estimate of service cost and/or notifying the user of at least some aspect of estimated service cost or projected service cost, providing the user with a UI for the purpose of providing the user with one or more service usage and/or service cost notification messages that require user acknowledgement and/or a user decision and obtaining or reporting the user acknowledgements and/or decisions, providing the user with a UI for the purpose of providing the user with service options and/or service payment options, providing the user with a UI for the purpose of obtaining user choice for such options when service usage or cost estimates are about to run over limits or have run over limits or are projected to run over limits, providing the user with a UI for the purpose of monitoring or conducting open central billing transactions or other transactions, providing the user with a UI for the purpose of selecting the service control techniques and/or policies and/or algorithms and/or pre-packaged configurations that can be used to define or partially define the service activity usage control policies implemented in the device service processor or the network service control equipment/billing system or a combination of both); service control for roaming on different networks that typically do not have compatible DPI-type techniques with the home network; certain service notification and traffic control algorithms (e.g., stack-ranked activity statistical analysis and control of only the high usage activities); and/or a function for assigning a device to a service experience or ambient activation experience or virtual service provider (VSP) at various times from manufacturing to device distribution to a user of the device. In some embodiments, certain activities are implemented in the device as a solution for networks in which a new centralized DPI approach is not possible, not economically feasible, or for any number of reasons not an option or not a preferred option.

[0272] In some embodiments, a network based solution is provided for a more basic set of services for all devices that do not have service control capabilities, and a super-set of services

and/or additional services are provided for devices that include a service processor. As described herein, a service controller function can be located in various places in the network in accordance with various embodiments. It should also be noted that various other embodiments described herein also employ a hybrid service control function performing certain service control functions in the network (e.g., collecting network service usage information, such as IPDRs, and/or performing DPI related functions in the network for collecting network service usage information and/or throttling/shaping traffic) and service control functions in the device (e.g., service processor 115, which, for example, monitors service usage in the device and/or performs throttling or traffic shaping in the device and/or performs certain billing event recording and reporting functions that are aptly performed on the device).

[0273] In some embodiments, lower level service policy implementation embodiments are combined with a higher level set of service policy supervision functions to provide device assisted verifiable network access control, authentication and authorization services.

[0274] In some embodiments, device based access control services are extended and combined with other policy design techniques to create a simplified device activation process and connected user experience referred to herein as ambient activation. As similarly discussed above, ambient activation can be provided by setting access control to a fixed destination, verifying access with IPDRs, verifying access by setting a max data rate and triggering off in the network if it exceeds the max data rate, and/or by various other techniques.

[0275] As shown in FIG. 16, service controller 122 includes a service history server 1650. In some embodiments, the service history server 1650 collects and records service usage or service activity reports from the Access Network AAA Server 1621 and the Service Monitor Agent 1696. For example, although service usage history from the network elements can in certain embodiments be less detailed than service history from the device, the service history from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is extremely difficult for a device error or compromise event on the device to compromise the network based equipment and software. For example, service history reports from the device can include various service tracking information, as similarly described above. In some embodiments, the service history server 1650 provides the

service history on request to other servers and/or one or more agents. In some embodiments, the service history server 1650 provides the service usage history to the device service history 1618. In some embodiments, for purposes of facilitating the activation tracking service functions (described below), the service history server 1650 maintains a history of which networks the device has connected to. For example, this network activity summary can include a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. As another example, this activity summary can further be analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.

[0276] As shown in FIG. 16, service controller 122 includes a policy management server 1652. In some embodiments, the policy management server 1652 transmits policies to the service processor 115 via the service control link 1653. In some embodiments, the policy management server 1652 manages policy settings on the device (e.g., various policy settings as described herein with respect to various embodiments) in accordance with a device service profile. In some embodiments, the policy management server 1652 sets instantaneous policies on policy implementation agents (e.g., policy implementation agent 1690). For example, the policy management server 1652 can issue policy settings, monitor service usage and, if necessary, modify policy settings. For example, in the case of a user who prefers for the network to manage their service usage costs, or in the case of any adaptive policy management needs, the policy management server 1652 can maintain a relatively high frequency of communication with the device to collect traffic and/or service measures and issue new policy settings. In this example, device monitored service measures and any user service policy preference changes are reported, periodically and/or based on various triggers/events/requests, to the policy management server 1652. In this example, user privacy settings generally require secure communication with the network (e.g., a secure service control link 1653), such as with the policy management server 1652, to ensure that various aspects of user privacy are properly maintained during such configuration requests/policy settings transmitted over the network. For example, information can be compartmentalized to service policy management and not communicated to other databases used for CRM for maintaining user privacy.

[0277] In some embodiments, the policy management server 1652 provides adaptive policy management on the device. For example, the policy management server 1652 can issue policy settings and objectives and rely on the device based policy management (e.g., service processor 115) for some or all of the policy adaptation. This approach can require less interaction with the device thereby reducing network chatter on service control link 1653 for purposes of device policy management (e.g., network chatter is reduced relative to various server/network based policy management approaches described above). This approach can also provide robust user privacy embodiments by allowing the user to configure the device policy for user privacy preferences/settings so that, for example, sensitive information (e.g., geo-location data, website history) is not communicated to the network without the user's approval. In some embodiments, the policy management server 1652 adjusts service policy based on time of day. In some embodiments, the policy management server 1652 receives, requests or otherwise obtains a measure of network availability and adjusts traffic shaping policy and/or other policy settings based on available network capacity.

[0278] In some embodiments, the policy management server 1652 performs a service control algorithm to assist in managing overall network capacity or application QoS. In some embodiments, the policy management server 1652 performs an algorithm to determine which access network is best to connect to, such as based on network capacity or application QoS, service usage costs, and/or any other criteria. In some embodiments, the device is capable of connecting to more than one network, and accordingly, device service policies can be selected/modified based on which network the device is connected to. In some embodiments, the network control plane servers detect a network connection change from a first network to a second network and initiate the service policy implementation established for the second network. In other embodiments, the device based adaptive policy control agent (e.g., policy control agent 1692 described herein) detects network connection changes from the first network to the second network and implements the service policies established for the second network.

[0279] In some embodiments, when more than one access network is available, the network is chosen based on which network is most preferred according to a network preference list or according to the network that optimizes a network cost function. For example, the preference list can be pre-established by the service provide and/or the user. For example, the

network cost function can be based on a minimum service cost, maximum network performance, determining whether or not the user or device has access to the network, maximizing service provider connection benefit, reducing connections to alternative paid service providers, and/or a variety of other network preference criteria. In other embodiments, the device detects when one or more preferred networks are not available, implements a network selection function or intercepts other network selection functions, and offers a connection to the available service network that is highest on a preference list. For example, the preference list can be set by the service provider, the user and/or the service subscriber.

[0280] As shown in FIG. 16, service controller 122 includes a network traffic analysis server 1656. In some embodiments, the network traffic analysis server 1656 collects/receives service usage history for devices and/or groups of devices and analyzes the service usage. In some embodiments, the network traffic analysis server 1656 presents service usage statistics in various formats to identify improvements in network service quality and/or service profitability. In other embodiments, the network traffic analysis server 1656 estimates the service quality and/or service usage for the network under variable settings on potential service policy. In other embodiments, the network traffic analysis server 1656 identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.

[0281] As shown in FIG. 16, service controller 122 includes a beta test server 1658. In some embodiments, the beta test server 1658 publishes candidate service plan policy settings to one or more devices. In some embodiments, the beta test server 1658 provides summary reports of network service usage or user feedback information for one or more candidate service plan policy settings. In some embodiments, the beta test server 1658 provides a mechanism to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further policy settings optimization.

[0282] As shown in FIG. 16, service controller 122 includes a service download control server 1660. In some embodiments, the service download control server 1660 provides a download function to install and/or update service software elements (e.g., the service processor 115 and/or agents/components of the service processor 115) on the device, as described herein.

[0283] As shown in FIG. 16, service controller 122 includes a billing event server 1662. In some embodiments, the billing event server 1662 collects billing events, provides service plan information to the service processor 115, provides service usage updates to the service processor 115, serves as interface between device and central billing server 1619, and/or provides trusted third party function for certain ecommerce billing transactions.

[0284] As shown in FIG. 16, the Access Network AAA server 1621 is in network communication with the access network 1610. In some embodiments, the Access Network AAA server 1621 provides the necessary access network AAA services (e.g., access control and authorization functions for the device access layer) to allow the devices onto the central provider access network and the service provider network. In some embodiments, another layer of access control is required for the device to gain access to other networks, such as the Internet, a corporate network and/or a machine to machine network. This additional layer of access control can be implemented, for example, by the service processor 115 on the device. In some embodiments, the Access Network AAA server 1621 also provides the ability to suspend service for a device and resume service for a device based on communications received from the service controller 122. In some embodiments, the Access Network AAA server 1621 also provides the ability to direct routing for device traffic to a quarantine network or to restrict or limit network access when a device quarantine condition is invoked. In some embodiments, the Access Network AAA server 1621 also records and reports device network service usage (e.g., device network service usage can be reported to device service history 1618).

[0285] As shown in FIG. 16, the device service history 1618 is in network communication with the access network 1610. In some embodiments, the device service history 1618 provides service usage data records used for various purposes in various embodiments. In some embodiments, the device service history 1618 is used to assist in verifying service policy implementation. In some embodiments, the device service history 1618 is used to verify service monitoring. In some embodiments, the device service history 1618 is used to verify billing records and/or billing policy implementation. In some embodiments, the device service history 1618 is used to synchronize and/or verify the local service usage counter.

[0286] As shown in FIG. 16, the central provider billing server 1619 is in network communication with the access network 1610. In some embodiments, the central provider billing server 1619 provides a mediation function for central provider billing events. For example, the central provider billing server 1619 can accept service plan changes. In some embodiments, the central provider billing server 1619 provides updates on device service usage, service plan limits and/or service policies. In some embodiments, the central provider billing server 1619 collects billing events, formulates bills, bills service users, provides certain billing event data and service plan information to the service controller 122 and/or device 100.

[0287] Establishing Coordinated Service and Verification Policies for Service Processor, Service Controller and Network Functions

[0288] In some embodiments, device and network apparatus coordinate one or more of the following: network service policy implementation settings, device service policy implementation settings, network service profile implementation settings, device service profile implementation settings, network service usage measures used for the purpose of verifying service policy implementation, device service usage measures used for the purpose of verifying service policy implementation, network actions taken upon detection of service usage policy violation and device actions taken upon detection of service usage policy violation. In some embodiments, local device settings for the service monitoring, usage and/or billing profile or policy settings used, for example, by a device service processor 115, are associated with corresponding records for the various network apparatus that also rely upon the service policy and profile settings to monitor, control and/or bill for services or to respond to out of policy service usage conditions. For example, such network apparatus include the service controller 122 or similar functions, the billing system 123 or similar functions, the network AAA 121, gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720, or other networking equipment. In some embodiments, the service profile or policy settings are associated between the device and network in a manner that allows for effective and coordinated operation between the device service processor 115 and the network apparatus, but does not require an explicit function that simultaneously controls/ coordinates the service policy or profile implementation and/or verification actions taken by the device 100 (e.g., the service processor 115) and the network

apparatus. As an example, such embodiments can be applied in overlay applications as discussed below.

[0289] In some embodiments, a network function (e.g., the service controller 122, and/or more specifically the policy management server 1652 function, or other similar function) obtain, derive or otherwise determine the association of the service profile or policy settings to program a device service processor 115 and the various network apparatus functions (e.g., possibly including but not limited to the service controller 122 or similar functions, the billing system 123 or similar functions, the network AAA 121, gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720, or other networking equipment) by reading, receiving, querying, pulling or otherwise obtaining the settings from one or more of the network apparatus functions or from a data base that stores the service policy or profile settings for one or more of the network apparatus functions. After obtaining one or more of the network apparatus settings, a mapping (e.g., an association) of the network apparatus settings to the appropriate device 100 (service processor 115) settings can be determined to advantageously support the service usage monitoring, service usage control, service usage billing or service usage verification objectives being addressed. The policy or profile settings for the device can be a direct translation of the policy or profile settings used for the network apparatus, or the device policy or profile settings can be less directly derived from the network apparatus policy or profile settings. For example, service usage limits contained in the billing system 123 service plan can be either directly mapped to usage limit settings on the device service processor 115 (e.g., service usage stops when the limit is hit or the user is notified or the user is billed), or the usage limits can be mapped to a number of service profiles the user may select from (e.g., as discussed herein, the user can select from options involving various actual usage versus usage limit notification policies and/or service usage control, limitations or throttling policies).

[0290] For example, the service usage policy or profile limits or allowances maintained for the network apparatus functions (e.g., the service profile or service plan usage limits stored in the billing system 123 or AAA 121) can be read or queried by a network function (e.g., the service controller 122 or the service controller 122 through a second intermediary server connected to the billing system 123 and/or the AAA system 121), and the service usage limits stored in these networking apparatus can be either directly translated to the settings for the

service processor 115 or may need to be interpreted, expanded or otherwise modified to obtain the required service processor 115 policy and/or profile settings.

[0291] In some embodiments, the service usage limits set in the billing system 123 service plan record, and/or the service profile record stored in the AAA system 121 can be acquired (e.g., from the apparatus or from a database storing the settings for the apparatus) by the service controller (or another network function) and directly translated and used to program the settings in the service processor 123. In some embodiments, the service usage limits are determined or obtained by the activation server apparatus embodiments, other apparatus embodiments associated with service activation, or the virtual service provider embodiments, as described herein. In this manner, once the association of the service usage profile or policy settings used by a device service processor 115 and the profile or policy settings used by the various network apparatus functions is established, then the service policy or profile for service monitoring, control, billing, verification and/or actions taken on verification error can be coordinated between device and network even if some of the network functions act independent of some of the device functions.

[0292] For example, associating the service usage policies and/or profiles between the device service processor 115 and the various network apparatus functions, and then allowing for independent operation or action by the various functions in a manner that results in a coordinated outcome, facilitates an overlay of the device assisted services technology onto existing network equipment in a manner that results in reliable and verifiable service enhancements while minimizing the need for major existing network equipment upgrades.

[0293] In some embodiments, the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings used by the various network apparatus functions can be provided by a centralized network function that determines the appropriate settings for the network apparatus and the service processor 115 and sets one or more settings to each function. In some embodiments, this networking function is provided by a centralized network management function or service account activation function (e.g., the activation server apparatus embodiments, one of the other disclosed apparatus

embodiments associated with service activation or the virtual service provider apparatus embodiments, as described herein).

[0294] In some embodiments, the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings used by the various network apparatus functions can be provided by a network function that by reads, receives, queries, pulls or otherwise obtains the setting used by the service controller 122 or the service processor 115. The network function can then determine the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings required by the various network apparatus functions before writing, transmitting, pushing, or otherwise recording the appropriate settings required by each of the other network apparatus functions. In some embodiments, this functionality can be implemented in the service controller (e.g., the policy management server, possibly acting in coordination with another network function or server), which then links into the databases used for storing the policy or profile settings for the other network apparatus.

[0295] In some embodiments, once the association is established between service policy or profile settings in the network apparatus and the service policy or profile settings in the service processor 115, then the network based service usage measures (e.g., IPDRs communicated to the billing system 123, the AAA 121, service controller 122 or other network functions used to verify service usage and/or take actions) used for verification of device 100 service usage versus service policy or profile can be monitored by the network apparatus (e.g., billing system 123 and AAA 121) independent of coordination with the service processor 115 and/or independent of the service controller 122. In some embodiments, in addition to independent monitoring and verification of service usage versus policy, independent service profile or policy verification error response actions can be taken by the network apparatus (e.g., suspend, quarantine, SPAN or flag device 100, notify the user and possibly require acknowledgement, or bill the user account for service usage overage) without direct involvement by the service processor 115 and/or the service controller 122.

[0296] Accordingly, the association between service profile and/or service policy that is implemented on the device 100 (e.g., service processor 115) and the service profile and/or policy

usage limits recorded in network apparatus can be associated with one another by one or more of the following: (A) implementing a function to read from the network database (e.g., the billing 123 data base, AAA 121 data base, service controller 122 data base, etc.) and mapping the network profiles and/or policies to device 100 (e.g., service processor 115) profiles and/or policies; (B) implementing a function that simultaneously sets the device profile and/or policy and the network equipment profile and/or policy recorded in the appropriate data base records; and (C) implementing a function that reads the profile and/or policy on the device 100 (e.g., service processor 115) or the service controller 122 and then sets the network equipment profile and/or policy recorded in the appropriate data base records. This allows for a simplified but coordinated response to monitoring, controlling and billing for service usage, for verifying service usage versus service usage profile or policy, and/or initiating or carrying out network actions in response to service usage versus profile or policy verification errors and/or device actions in response to service usage versus profile or policy verification errors.

[0297] FIG. 17 is another functional diagram illustrating the device based service processor 115 and the service controller 122 in accordance with some embodiments. FIG. 17 provides for various embodiments as similarly described above with respect to the various embodiments described above with respect to FIG. 16, with one of the differences being that the service controller 122 as shown in FIG. 17 is connected to the access network and not (directly) connected to the Internet. Accordingly, as shown in FIG. 17, in some embodiments, the service control link 1653 is a communications link between the service controller 122 and the service processor 115 over the access network 1610.

[0298] FIG. 18 is another functional diagram illustrating the device based service processor 115 and the service controller 122 in which the service processor controls the policy implementation for multiple access network modems and technologies in accordance with some embodiments. As shown, FIG. 18 provides for various embodiments as similarly described above with respect to the various embodiments described above with respect to FIG. 16, with one of the differences being that the service processor controls the policy implementation for multiple access network modems and technologies. Accordingly, as shown in FIG. 18, in some embodiments, a connection manager 1804, which as shown is in control plane communication with a modem selection and control 1811, provides a control and supervision function for one or

more modem drivers or modems that connect to an access network. In some embodiments, the modem selection and control 1811 selects the access network connection and is in communication with the modem firewall 1655, and modem drivers, which as shown include Dial/DSL modem driver 1831, Ethernet modem driver 1815, WPAN modem driver 1814, WLAN modem driver 1813, and WWAN modem driver 1812, convert data traffic into modem bus traffic for one or more modems and are in communication with the modem selection and control 1811.

[0299] FIG. 19 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. As shown in FIG. 19, a stripped down (e.g., reduced set of agents/components/functionality) embodiment of the service processor 115 and the service controller 122 are provided in which service policy is not adaptive but rather is set by the service controller 122. In this example, the agent within the service processor 115 that implements service policy is the policy implementation agent 1690. Also, in this example, the service controller 122 is similarly stripped down to a simplified configuration (e.g., reduced set of agents/components/functionality).

[0300] Referring to FIG. 19, in some embodiments, many of the service policy implementation verification and compromise protection techniques are similarly provided using these simplified configurations of the service processor 115 and the service controller 122, as described above with respect to, for example, FIG. 16. For example, the service control device link 1691 and service control server link 1638 can be used for downloading service policies to the policy implementation agent 1690 (but, in some embodiments, cannot perform the heartbeat or authentication function).

[0301] For example, a basic service profile or service policy implementation verification technique for this reduced configuration calls for the access control integrity server 1654 to obtain IPDRs from access network AAA server 1621 (or 121) (e.g., or other network functions as described herein) and compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the access control integrity server 1654 initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed

herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0302] In some embodiments, a service profile or service policy implementation verification technique for this reduced configuration calls for the billing system 123 to obtain IPDRs from access network AAA server 1621 (or 121) (or other network functions as discussed herein) and compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the billing system 123 initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0303] In some embodiments, a service profile or service policy implementation verification technique for this reduced configuration calls for the AAA server 1621 (or 121) itself to compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the AAA server 1621 (or 121) initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0304] Accordingly, this approach provides a basic first layer of service policy implementation verification that does not depend on device based agent behavior for the verification. If the service policy is in error in a way that violates the expected service policy usage limits, then the access control integrity server 1654 will detect this condition and appropriate action can be taken. In some embodiments, if one or more service policy integrity verification tests fail, the appropriate responsive actions can include routing the device to quarantine status, sending an error message to the device or device user interface and then suspend access for the device, and/or limiting access in some way without completely suspending access, as similarly described above. In some embodiments, if one or more service policy integrity verification tests fail, the appropriate responsive actions can include logging excess service usage above the intended service policy limits and billing the user for some or all of the excess usage, sending the user a notification and/or acknowledgement response request (possibly including a simple keystroke acknowledgement, or a password, a biometric signature or other secure response), and/or limiting access in some way without completely suspending access, as similarly described above.

[0305] In some embodiments, a billing system technique provides another verification overlay. For example, the service processor 115 can have a set of service policy implementations (or service profile) that calls for maintaining service usage within a certain limit, or assisting the user or network to maintain service usage to that limit. The billing system 123 can be implemented in a way to provide a “back stop” to the service usage controls or limits provided for by the service processor 115, so that even if the service processor 115 is compromised, hacked, spoofed or is otherwise in error, the billing system 123 protects the service provider, “service owner”, carrier, VSP or network operator from unpaid access beyond the service limits. This can be accomplished, for example, by assigning a service usage limit within the billing system 123 so that if the service processor 115 is compromised and the service usage runs over the desired limit, the billing system 123 automatically charges the user account for the overage. The billing system 123 can receive service usage information from the IPDRs that are aggregated in the network as in the case of a conventional billing system, and because these network based measures are independent from the device agent operation, they cannot be spoofed by merely spoofing something on the device or service processor 115. In this manner, defeating the service processor 115 service agent control mechanisms described herein simply

results in a billing charge and not free service. In some embodiments, if the service usage runs over the service usage limit specified in the service profile, the user can be notified as discussed herein, and the user can be required to acknowledge the overage and approve a billing charge for the overage as also discussed herein, with the acknowledgement being communicated back to the network in some embodiments. This positive acknowledgement also provides a layer of protection and verification of the service control and usage limit control for the device service processor 115. In some embodiment also discussed herein, the user is requested to input a password, biometric or other secure response to the usage overage notification, providing yet another layer of protection to verify that the user intends to pay for the service usage overage. In these embodiments taken individually or in combination, the service processor 115 assistance for service usage control can be verified and/or protected from compromise.

[0306] In some embodiments, the service control device link 1691 and service control server link 1638 are used to implement the service processor 115 heartbeat authentication and communication functions to strengthen the verification of a proper service policy implementation of the embodiments of FIG. 19. For example, the heartbeat function can be used as authentication for service monitoring versus network reports. In addition, the heartbeat function can be used as authentication for challenge/response queries of agents. Also, the heartbeat function can be used as authentication for access control. In some embodiments, to strengthen verification of the basic system illustrated in FIG. 19, the communication access to the policy implementation agent 1690 is restricted so that software or hardware on device 100 and/or on a network cannot have authorized access to the policy implementation agent 1690. For example, authorized access to the policy implementation agent 1690 can be restricted to include only the service controller 122 through the service control device link 1691 and the service control server link 1638. For example, the agent control bus 1630 can be secured with encryption and/or other security techniques so that only the service control device link 1691 can have authorized access to the policy implementation agent 1690. As another example, the agent level message encryption can be used as described herein.

[0307] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened against errors, intrusion, tampering, hacking and/or other inadvertent or intentional integrity degradation by using various other techniques.

For example, the dynamic agent download feature of the service controller 122 can download a new version of the policy implementation agent 1690. In this example, the new agent code can be identical in functionality and also hashed, obfuscated or ordered differently before signing and encryption so that any hacking attempt must be reinitiated, and this process can be periodically repeated or repeated upon a triggering event. Additionally, once the new dynamically loaded agent is in place, it can be required to perform an environment scan to determine if the system configuration or operation are as expected, and/or it can seek to detect elements in the execution environment that can be harmful or threatening to the integrity of the policy implementation. The agent can also be required to report back on the scan within a relatively short period of time so that any attempt to compromise the agent does not have sufficient time to be effective.

[0308] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened to protect the policy implementation from compromise attempts by locating the software and/or hardware used onto an access modem associated with the service. For example, the modem can make it difficult to get access to the policy implementation agent 1690 by employing one or more security elements on one or more access ports into the modem, such as the device bus, an I/O port, a network connection or the debug port. The modem can also store and/or execute the policy implementation agent in secure memory. The modem can also require a secure download key or a secure software signature to accept any updates to the agent software.

[0309] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened against compromise attempts by performing scans of the device 100 code execution environment and/or code storage environment to identify potentially malicious and/or unwanted/untrusted software or hardware. For example, this function can be performed by the policy implementation agent 1690. The agent can have a local database of potentially malicious elements and compare the entries in the database against the elements detected locally using various malicious code, behavior blocking, intrusion detection, and/or other well known techniques for security analysis. Alternatively or in addition, the agent can communicate a list of some or all of the elements detected locally to the service controller 122 to augment or take the place of the database comparison function that can be performed locally, thereby performing such or further such security analysis on the network (e.g., by the

service controller 122), and, in some embodiments, if not automatically detected, such elements detected locally (e.g., and/or samples of such detected potentially malicious code or logs of potentially malicious/suspicious behavior/intrusions) forwarded to security analysts for the service provider for further security analysis (e.g., service provider security analysts and/or an outside security vendor engaged to protect the service provider's network and supported devices). In some embodiments, the agent detects new software downloads, installs and/or invocations and immediately issues an error flag report when potentially malicious software is downloaded, installed or invoked (e.g., file and network based on access security detection techniques). In some embodiments, the agent scans the local software loading and invocation activity along with a log of other software runtime events and regularly reports this trace so that when an error or compromise event occurs the trace preceding the event can be analyzed to determine the offending software or activity trace that took place to cause the compromise or error. For example, once the software or activity that caused the compromise is known or otherwise detected, it can be entered into a refreshed version of the database that the device and other devices use to detect potentially malicious precursor conditions. Examples of such precursor events can include software invocations, software downloads, a sequence of memory I/O events, a sequence of software access events, a sequence of network address or URL communications or downloads, or a sequence of access modem I/O activity.

[0310] FIG. 20 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. As shown in FIG. 20, the modem firewall 1655 has been removed, and firewall and access control and traffic shaping functions are performed in these embodiments by the policy implementation agent 1690 and application interface agent 1693.

[0311] FIG. 21 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. FIG. 21 illustrates the various modem drivers and modems 2122 through 2125 and 2141. In some embodiments, the modems, which include WWAN modem 2122, WLAN modem 2123, WPAN modem 2124, Ethernet modem 2125, and Dial/DSL modem 2141, which are in communication with the modem bus 2120, connect the device to one or more networks. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent

1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation agent 1690, or, in some embodiments, the modem firewall agent 1655 or the application interface agent 1693, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult or impossible to make a complete determination of traffic parameters. It should be noted that although the present invention does not need to implement any or all of the measurement points illustrated in FIG. 21 to have an effective implementation as was similarly shown with respect to FIG. 19, various embodiments benefit from these and/or similar measurement points. It should also be noted that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation.

[0312] As shown in FIG. 21, measurement point I occurs at the application interface agent 1693 interface to the applications. At this measurement point, the application traffic can be monitored before it is framed, packetized or encrypted by the lower layers of the networking stack. For example, this allows inspection, characterization, tagging (literal or virtual) and, in some embodiments, shaping or control of services or traffic. At this measurement point, traffic can be more readily associated with applications, URLs or IP addresses, content type, service type, and other higher level parameters. For example, at this level email traffic and downloads, web browser applications and end points, media file transfers, application traffic demand, URL traffic demand and other such service monitoring parameters are more readily observed (e.g., accessible in the clear without the need for deep packet inspection and/or decryption), recorded and possibly shaped or controlled. As described herein, it is also possible to monitor upstream traffic demand at this point and compare it to the other measurement points to determine if the traffic policies in place are meeting overall traffic control policy objectives or to determine if traffic policy implementation is operating properly. For example, the downstream delivered traffic can be optimally observed at this measurement point.

[0313] As shown in FIG. 21, traffic measurement points II and III are situated on the upstream and downstream sides of policy implementation agent 1690. As described herein, these two locations allow potential tracking of upstream and downstream traffic through the stack portions associated with the policy implementation agent 1690. These two locations also provide for potential cross-checking of how the policy implementation agent 1690 is impacting the demand and delivery of traffic. In a similar manner, measurement point III in connection with measurement point IV provide an opportunity for packet tracing through the stack components associated with the modem firewall 1655 and provide for the opportunity to observe the demand and delivery sides of the modem firewall 1655. Traffic measurement point V provides the potential for observing the traffic at the modem bus drivers for each of the modems.

[0314] As shown in FIG. 21, traffic measurement point VI provides, in some embodiments, the ultimate measure of access traffic, for example, the traffic that actually transacts over the access network through the modem. As shown, measurement point VI is at the modem side of the internal or external communications bus 1630, and it will be appreciated that, in some embodiments, this measurement point can be further down the modem stack closer to the MAC or physical layer (e.g., at the designer's discretion). An advantage of having a measurement point deep in the modem is, for example, that if the software or hardware that implements the measurement and reporting is well secured against compromise, then this measure can be almost as strong from a verification perspective as the measure that comes from the network (e.g., from the network elements). Accordingly, this makes it possible to compare this measure against the other measures to determine if there is a traffic path that is leaking past the other measurement point or one or more policy implementation points.

[0315] FIGS. 22A and 22B provide tables summarizing various service processor 115 agents (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments. Many of these agents are similarly described above, and the tables shown in FIGS. 22A and 22B are not intended to be an exhaustive summary of these agents, nor an exhaustive description of all functions that the agents perform or are described herein, but rather FIGS. 22A and 22B are provided as a summary aid in understanding the basic functions of each agent in accordance with some embodiments and how the agents interact with one another,

with the service controller server elements, and/or with other network functions in certain embodiments to form a reliable device based service delivery solution and/or platform.

[0316] FIG. 23 provides a table summarizing various service controller 122 server elements (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments. Many of these agents are similarly described above, and the table shown in FIG. 23 is not intended to be an exhaustive summary of these server elements, nor an exhaustive description of all functions that the elements perform or are described herein, but rather FIG. 23 is provided as a summary aid in understanding the basic functions of each element in accordance with some embodiments and how the elements interact with one another, certain network elements, and/or the service processor agents in certain embodiments to form a reliable device based service delivery solution and/or platform.

[0317] In some embodiments, it is desirable to provide a control plane between the service processor and the service controller using a flexible connection or communication path that, for example, will work between virtually any two network connection endpoints, one being the service controller and one being the device, in a secure yet scalable manner. In view of the embodiments described herein, one of ordinary skill in the art will recognize that it is possible to achieve such features with a variety of different embodiments that share similar core features to the embodiments described herein.

Service Control Device Link and Continuous Heartbeat Authentication

[0318] As described herein, there are numerous ways to implement the control plane communication channel between the service processor 115 and the service controller 122. Various embodiments described herein disclose a secure and bandwidth efficient control plane that is compatible with any IP based network (including the ability to locate the service controller 122 over the Internet); provides for consistent device assisted service monitoring, control, verification and/or billing while roaming across multiple networks with different access technologies; and allows continuous device assisted service control verification and/or authentication with a variety of mechanisms for setting the transmission heartbeat frequency. Other techniques that could be used for this function include, for example, encapsulating the control plane in the access network control plane channel, encapsulating the control plane in IP

or data packet framing mechanisms (e.g., IPV6), running a more conventional VPN or IPSEC channel, and/or using an independent access network connection.

[0319] FIG. 24 is a functional diagram illustrating the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 in accordance with some embodiments. In particular, the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 as shown in FIG. 24 provide for secure control plane communication over the service control link 1653 between the service processor 115 and the service controller 122 in accordance with some embodiments. Various embodiments include two or three layers of encryption in the service control link, with one embodiment or layer being implemented in the encrypt functions (2408, 2428) and decode functions (2412, 2422), and another embodiment or layer implemented in the transport services stack (2410, 2420). An optional third embodiment or layer of encryption is implemented below the transport services stack, for example, with IPSEC or another IP layer encryption, VPN or tunneling scheme. For example, various known security encryption techniques can be implemented in the encrypt functions (2408, 2428), with public/private or completely private keys and/or signatures so that very strong levels of security for service processor control plane traffic can be achieved even through the basic transport services (2410, 2420) implemented with standard secure or open Internet networking protocols, such as TLS or TCP. For example, the service processor agent communications local to the device can be conducted to and from the service controller elements via the service control device link 1691 connection to the agent communication bus 1630. The combination of the service control device link 1691 and the agent communication bus 1630, which in some embodiments is also securely encrypted or signed, provides a seamless, highly secure, asynchronous control plane connection between the service processor and service controller server elements and the service controller and service controller agents that works over a wide range of access networks, such as any access network that has the capability to connect IP or TCP traffic to another TCP or IP endpoint on the access network, another private network or over the Internet 120. As described herein, in some embodiments, the agent communication bus 1630 also provides a fourth level of encrypted or signed communication to form a secure closed system on the device for agent to agent communication, for example, making it very difficult or practically impossible for software or applications to gain access to one or more of the a service processor agents on the device in any

way other than the service control device link 1691. In this way, in some embodiments, the agent communication bus 1630 and the service processor agents can only be accessed by one another as necessary or permitted by agent communication policies, or by the service controller or other authorized network function with proper security credentials communicating over the service control device link 1691. Additionally, in some embodiments, communications between a subset of two or more agents, or between one or more agents and one or more service controller server elements are encrypted with unique keys or signatures in such a way that a fourth level of security providing private point to point, point to multipoint, or multipoint to multipoint secure communication lines is provided.

[0320] In some embodiments, all of the service control device link 1691 communications are transformed into a continuous control plane connection, with a frequency based on the rate of service usage, a minimum set period between connections, and/or other methods for establishing communication frequency. In some embodiments, this heartbeat function provides a continuous verification link by which the service controller verifies that the service processor and/or device are operating properly with the correct service policies being implemented. In view of the following heartbeat function embodiments described herein, it will be apparent to one of ordinary skill in the art that different approaches for implementing the various heartbeat embodiments are possible, and it will be clear that there are many ways to achieve the essential features enabling a reliable, sometimes continuous control link and verification function for the purpose of assisting control of service usage in a verifiable manner. As shown, inside the service processor 115, the service control device link 1691 includes a heartbeat send counter 2402 in communication with the agent communication bus 1630. For example, the heartbeat send counter 2402 can provide a count for triggering when a service processor 115 communication (e.g., periodic communication based on a heartbeat mechanism) should be sent to the service controller 122, and a heartbeat buffer 2404, also in communication with the agent communication bus 1630, buffers any such information for the next service processor 115 communication, in accordance with various heartbeat based embodiments, as similarly described herein. The heartbeat buffer 2404 is in communication with a framing element 2406 and an encrypt element 2408 for framing and encrypting any service processor 115 communications transmitted to the service controller 122 by a transport services stack 2410 over the service control link 1653. Similarly, as shown inside the service controller 122, the service control

server link 1638 includes a heartbeat send counter 2434 in communication with a service controller network 2440, a heartbeat buffer 2432, also in communication with the service controller network 2440, buffers any such information for the next service controller 122 communication, in accordance with various heartbeat based embodiments, as similarly described herein. The heartbeat buffer 2432 is in communication with a framing element 2430 and an encrypt element 2428 for framing and encrypting any such service controller 122 communications transmitted to the service processor 115 by a transport services stack 2420 over the service control link 1653.

[0321] As also shown inside the service processor 115 of FIG. 24, the service control device link 1691 includes a decode element 2412 for decoding any received service controller 122 communications (e.g., decrypting encrypted communications), an unpack element 2414 for unpacking the received service controller 122 communications (e.g., assembling packetized communications), and an agent route 2416 for routing the received service controller 122 communications (e.g., commands, instructions, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent refreshes and/or new software for installation) to the appropriate agent of the service processor 115. Similarly, as shown inside the service controller 122, the service control server link 1638 also includes a decode element 2422 for decoding any received service processor 115 communications (e.g., decrypting encrypted communications), an unpack element 2424 for unpacking the received service processor 115 communications (e.g., assembling packetized communications), and an agent route 2426 for routing the received service processor 115 communications (e.g., responses to instructions and/or commands, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent status information, network service/cost usage and/or any other reporting related information) to the appropriate agent of the service controller 122. Accordingly, as described herein with respect to various embodiments, the various secure communications between the service controller 122 and the service processor 115 can be performed using the embodiment as shown in FIG. 24, and those of ordinary skill in the art will also appreciate that a variety of other embodiments can be used to similarly provide the various secure communications between the service controller 122 and the service processor 115 (e.g., using different software and/or hardware architectures to provide secure communications, such

as using additional and/or fewer elements/functions or other design choices for providing such secure communications).

[0322] In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided, and the following embodiments (e.g., as shown and described with respect to FIG. 25) teach such a structure that packs the various service processor agent control plane communications and the various service controller element control plane connections into a format that does not consume excessive bandwidth to enable a continuous control plane connection between the device and service controller. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to buffer such communication messages for some period of time before framing and transmitting, such as in a heartbeat frequency that is based on rate of service usage. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to allow for the frame to be easily packed, encrypted, decoded, unpacked and the messages distributed. In view of the various embodiments described herein, it will be apparent to one of ordinary skill in the art that many framing structures will work for the intended purpose of organizing or framing agent communications and the uniqueness and importance of combining such a system element with the device service controller functions, the service processor functions, the service control verification functions and/or the other purposes.

[0323] FIG. 25 is a functional diagram illustrating a framing structure of a service processor communication frame 2502 and a service controller communication frame 2522 in accordance with some embodiments. In particular, the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 (e.g., as shown in FIG. 24) provide for secure control plane communication over the service control link 1653 between the service processor 115 and the service controller 122 using communication frames in the format of the service processor communication frame 2502 and the service controller communication frame 2522 as shown in FIG. 25 in accordance with some embodiments. As shown, the service processor communication frame 2502 includes a service processor framing sequence number 2504, a time stamp 2506, an agent first function ID 2508, an agent first function message length 2510, an agent first function message 2512, and assuming

more than one message is being transmitted in this frame, an agent Nth function ID 2514, an agent Nth function message length 2516, and an agent Nth function message 2518. Accordingly, the service processor communication frame 2502 can include one or more messages as shown in FIG. 25, which can depend on networking frame length requirements and/or other design choices. Similarly, as shown, the service controller communication frame 2522 includes a service controller framing sequence number 2524, a time stamp 2526, an agent first function ID 2528, an agent first function message length 2530, an agent first function message 2532, and assuming more than one message is being transmitted in this frame, an agent Nth function ID 2534, an agent Nth function message length 2536, and an agent Nth function message 2538. Accordingly, the service controller communication frame 2522 can include one or more messages as shown in FIG. 25, which can depend on networking frame length requirements and/or other design choices.

[0324] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters (e.g., implemented by various agents, components, and/or functions implemented in software and/or hardware) in accordance with some embodiments. Many of these heartbeat functions and parameters are similarly described above, and the tables shown in FIGS. 26A-26H are not intended to be an exhaustive summary of these heartbeat functions and parameters, but rather are provided as an aid in understanding these functions and parameters in accordance with some heartbeat based embodiments described herein.

[0325] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments. Many of these device based service policy implementation verification techniques are similarly described above, and the tables shown in FIGS. 27A-27P are not intended to be an exhaustive summary of these device based service policy implementation verification techniques, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

[0326] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments. Many of these techniques for protecting the device based service policy from

compromise are similarly described above, and the tables shown in FIGS. 28A-28E are not intended to be an exhaustive summary of these techniques for protecting the device based service policy from compromise, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

Device Assisted Service Control and Traffic Control

[0327] As described below, various techniques are disclosed for implementing device assisted traffic shaping and service control at the lower levels of service usage policy implementation.

[0328] FIG. 29 is a functional diagram illustrating a device communications stack that allows for implementing verifiable traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. As shown, several service agents take part in data path operations to achieve various data path improvements, and, for example, several other service agents can manage the policy settings for the data path service, implement billing for the data path service, manage one or more modem selection and settings for access network connection, interface with the user and/or provide service policy implementation verification. Additionally, in some embodiments, several agents perform functions to assist in verifying that the service control or monitoring policies intended to be in place are properly implemented, the service control or monitoring policies are being properly adhered to, that the service processor or one or more service agents are operating properly, to prevent unintended errors in policy implementation or control, and/or to prevent tampering with the service policies or control. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent 1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation agent 1690, or in some embodiments the modem firewall agent 1655 or the application interface agent 1693, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult

or impossible to make a complete determination of traffic parameters. For example, a detailed set of embodiments describing how the various measurement points can be used to help strengthen the verification of the service control implementation are described herein, including, for example, the embodiments described with respect to FIG. 16 and FIG. 21. The particular locations for the measurement points provided in these figures are intended as instructional examples, and other measurement points can be used for different embodiments, as will be apparent to one of ordinary skill in the art in view of the embodiments described herein. Generally, in some embodiments, one or more measurement points within the device can be used to assist in service control verification and/or device or service troubleshooting.

[0329] In some embodiments, the service monitor agent and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through the various communication stack formatting, processing and encryption steps, and providing the virtual tag information to the various agents that monitor, control, shape, throttle or otherwise observe, manipulate or modify the traffic. This tagging approach is referred to herein as virtual tagging, because there is not a literal data flow, traffic flow or packet tag that is attached to flows or packets, and the book-keeping to tag the packet is done through tracking or tracing the flow or packet through the stack instead. In some embodiments, the application interface and/or other agents identify a traffic flow, associate it with a service usage activity and cause a literal tag to be attached to the traffic or packets associated with the activity. This tagging approach is referred to herein as literal tagging. There are various advantages with both the virtual tagging and the literal tagging approaches. For example, it can be preferable in some embodiments to reduce the inter-agent communication required to track or trace a packet through the stack processing by assigning a literal tag so that each flow or packet has its own activity association embedded in the data. As another example, it can be preferable in some embodiments to re-use portions of standard communication stack software or components, enhancing the verifiable traffic control or service control capabilities of the standard stack by inserting additional processing steps associated with the various service agents and monitoring points rather than re-writing the entire stack to correctly process literal tagging information, and in such cases, a virtual tagging scheme may be desired. As yet another example, some standard communication stacks provide for unused, unspecified or otherwise available bit fields in a packet frame or flow, and these unused, unspecified or otherwise available bit fields can be used to literally tag traffic without the need to

re-write all of the standard communication stack software, with only the portions of the stack that are added to enhance the verifiable traffic control or service control capabilities of the standard stack needing to decode and use the literal tagging information encapsulated in the available bit fields. In the case of literal tagging, in some embodiments, the tags are removed prior to passing the packets or flows to the network or to the applications utilizing the stack. In some embodiments, the manner in which the virtual or literal tagging is implemented can be developed into a communication standard specification so that various device or service product developers can independently develop the communication stack and/or service processor hardware and/or software in a manner that is compatible with the service controller specifications and the products of other device or service product developers.

[0330] It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in FIG. 29 is not required to have an effective implementation, such as was similarly shown with respect to various embodiments described herein, such as with respect to FIGS. 19 and 21, various embodiments can benefit from these and/or similar measurement points. It will also be appreciated that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation. In some embodiments, one or more measurement points are provided deeper in the modem stack (e.g., such as for embodiments similarly described herein with respect to FIGS. 35 and 36) where, for example, it is more difficult to circumvent and can be more difficult to access for tampering purposes if the modem is designed with the proper software and/or hardware security to protect the integrity of the modem stack and measurement point(s).

[0331] Referring to FIG. 29, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Example measurement point VI resides within or just above the modem driver layer. For example, the modem driver performs modem bus communications, data protocol translations, modem control and configuration to interface the networking stack traffic to the modem. As shown, measurement point VI is common to all modem drivers and modems,

and it is advantageous for certain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent tampering of the service controls. In some embodiments, the modem firewall is implemented farther up the stack, possibly in combination with other layers as indicated in other figures. In some embodiments, a dedicated firewall function or layer is provided that is independent of the other processing layers, such as the policy implementation layer, the packet forwarding layer and/or the application layer. In some embodiments, the modem firewall is implemented farther down the stack, such as within the modem drivers, below the modem drivers, or in the modem itself. Example measurement point IV resides between the modem firewall layer and an IP queuing and routing layer. As shown, an IP queuing and routing layer is separate from the policy implementation layer where the policy implementation agent implements a portion of the traffic control and/or service usage control policies. As described herein, in some embodiments, these functions are separated so that a standard network stack function can be used for IP queuing and routing, and the modifications necessary to implement the policy implementation agent functions can be provided

in a new layer inserted into the standard stack. In some embodiments, the IP queuing and routing layer is combined with the traffic or service usage control layer. Examples of this combined functionality are shown and described with respect to FIGS. 31, 32 and 33. For example, a combined routing and policy implementation layer embodiment can also be used with the other embodiments, such as shown in FIG. 29. Various detailed embodiments describing how the policy implementation layer can control traffic or other service usage activities are described with respect to FIG. 38. Measurement point III resides between the IP queuing and routing layer and a policy implementation agent layer. Measurement point II resides between the policy implementation agent layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 29.

[0332] As shown, the application service interface layer is above the standard networking stack API and, in some embodiments, its function is to monitor and in some cases intercept and process the traffic between the applications and the standard networking stack API. In some embodiments, the application service interface layer identifies application traffic flows before the application traffic flows are more difficult or practically impossible to identify farther down in the stack. In some embodiments, the application service interface layer in this way assists application layer tagging in both the virtual and literal tagging cases. In the case of upstream traffic, the application layer tagging is straight forward, because the traffic originates at the application layer. In some downstream embodiments, where the traffic or service activity classification relies on traffic attributes that are readily obtainable, such as source address or URL, application socket address, IP destination address, time of day or any other readily obtained parameter, the traffic type can be identified and tagged for processing by the firewall agent or another agent as it initially arrives. In other embodiments, as described herein, in the downstream case, the solution is generally more sophisticated when a traffic parameter that is needed to classify the manner in which the traffic flow is to be controlled or throttled is not readily available at the lower levels of the stack, such as association with an aspect of an

application, type of content, something contained within TLS, IPSEC or other secure format, or other information associated with the traffic. Accordingly, in some embodiments the networking stack identifies the traffic flow before it is fully characterized, categorized or associated with a service activity, and then passes the traffic through to the application interface layer where the final classification is completed. In such embodiments, the application interface layer then communicates the traffic flow ID with the proper classification so that after an initial short traffic burst or time period the policy implementation agents can properly control the traffic. In some embodiments, there is also a policy for tagging and setting service control policies for traffic that cannot be fully identified with all sources of tagging including application layer tagging.

[0333] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630, communicates user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or configuration information via this communications bus 1630, as shown (illustrating such communications with a reference (B) via the application layer, policy implementation agent layer, which is lower in the communications stack as shown, and/or the modem firewall layer). The connection manager agent communicates select and control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C) via the modem selection and control layer). Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (D) at the application layer, (E) at the policy implementation agent layer, and (F) at the modem firewall layer).

[0334] As shown in FIG. 29, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through VI, receiving information including application information, service usage and other service related information, and assignment information. An access

control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown.

[0335] In some embodiments, one or more of the networking stack modifications described herein in combination one or more of the service verification and tamper prevention techniques described herein is provided. As similarly described with respect to FIG. 29, the various example embodiments for assisting service control verification described herein and as summarized in the example tables provided in FIGS. 26, 27 and 28 can be employed individually or in combination to create increasingly secure cross-functional service control verification embodiments. In FIG. 29, the presence of the access control integrity agent, policy control agent, service monitor agent and the other agents that perform verification and/or tamper prevention functions illustrates verifiable service control aspects in accordance with some embodiments. Furthermore, the presence of the billing agent combined with the service verification and/or tamper prevention agents and techniques described herein provides for a set of verifiable billing embodiments for service billing, service billing offset corrections, bill by account, transaction billing and other billing functions. In addition, the presence of the user service interface agent in combination with the service control agent functions in the modified networking stack provide for embodiments involving a combination of service control with user preferences, which as described herein, provides the user with the capability to optimize service versus service cost in a network neutral manner. In some embodiments, the user control of service control policy is provided along with the service control verification and/or tamper prevention. The presence of the policy control agent that in some embodiments implements a higher than most basic level of policy decision and control with the policy implementation agents in the modified networking stack allows for, for example, the device to possess the capability to implement a higher level of service control for the purpose of obtaining a higher level service usage or service activity objective. In some embodiments, the application layer tagging in combination with other embodiments described herein provides for deep service activity control that is verifiable.

[0336] In some embodiments, verifiable traffic shaping as described herein can be performed using the device communications stack in a variety of embodiments for the combination of service control within the networking stack and service control verification

and/or tamper prevention, with various embodiments depicted in FIGS. 29 through 37. Additional levels of detail regarding how such embodiments can be used to implement verifiable traffic shaping are provided in and described with respect to FIGS. 38 through 40 which depict example functional diagrams of packet processing flows for verifiable traffic shaping or service activity control in a device service processor for both upstream and downstream flows. Along with several other interesting features embodied in FIGS. 38 through 40, application traffic layer tagging is depicted in additional detail in accordance with some embodiments. For example, the application interface agent can determine service data usage at the application layer using measurement point I and a local service usage counter, and can, for example, pass this information to the service monitor agent. If service usage exceeds a threshold, or if using a service usage prediction algorithm results in predicted service usage that will exceed a threshold, then the user can be notified of which applications are causing the service usage overrun or potential service usage overrun, via the user service interface agent. The user can then identify which application service (e.g., traffic associated with a specified high service use or non-critical application, such as for example a high bandwidth consumption social networking website or service, media streaming website or service, or any other high bandwidth website or service transmitting and/or receiving data with the service network) that the user prefers to throttle. As another example, the user could select a service policy that allows for video chat services until those services threaten to cause cost over-runs on the user's service plan, and at that time the service policy could switch the chat service to voice only and not transmit or receive the video. The traffic associated with the user specified application can then be throttled according to user preference input. For example, for downstream traffic, packets (e.g., packets that are virtually or literally tagged and/or otherwise associated with the application traffic to be throttled) from the access network can be buffered, delayed and/or dropped to throttle the identified application traffic. For upstream traffic, packets (e.g., packets that are virtually or literally tagged and/or otherwise associated with the application traffic to be throttled) can be buffered, delayed and/or dropped before being transmitted to the access network to throttle the identified application traffic. As similarly described above, traffic shaping as described herein can be verified, such as by the service monitor agent via the various measurement points and/or using other agents.

[0337] The embodiments depicted in FIG. 30 and other figures generally require enhancements to conventional device networking communication stack processing. For

example, these enhancements can be implemented in whole or in part in the kernel space for the device OS, in whole or in part in the application space for the device, or partially in kernel space and partially in application space. As described herein, the networking stack enhancements and the other elements of the service processor can be packaged into a set of software that is pre-tested or documented to enable device manufacturers to quickly implement and bring to market the service processor functionality in a manner that is compatible with the service controller and the applicable access network(s). For example, the service processor software can also be specified in an interoperability standard so that various manufacturers and software developers can develop service processor implementations or enhancements, or service controller implementations or enhancements that are compatible with one another.

[0338] FIG. 30 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, a portion of the service processor is implemented on the modem (e.g., on modem module hardware or modem chipset) and a portion of the service processor is implemented on the device application processor subsystem. It will be apparent to one of ordinary skill in the art that variations of the embodiment depicted in FIG. 30 are possible where more or less of the service processor functionality is moved onto the modem subsystem or onto the device application processor subsystem. For example, such embodiments similar to that depicted in FIG. 30 can be motivated by the advantages of containing some or all of the service processor network communication stack processing and/or some or all of the other service agent functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard feature set contained in a modem chipset hardware or software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

[0339] Referring to FIG. 30, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a

communication layer for modem MAC/PHY layer at the bottom of the device communications stack. Measurement point IV resides above the modem MAC/PHY layer. The modem firewall layer resides between measurement points IV and III. In the next higher layer, the policy implementation agent is provided, in which the policy implementation agent is implemented on the modem (e.g., on modem hardware). Measurement point II resides between the policy implementation agent and the modem driver layer, which is then shown below a modem bus layer. The next higher layer is shown as the IP queuing and routing layer, followed by the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 30.

[0340] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communicates user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent B communicates service settings and/or configuration information via this communications stack, as shown (illustrating such communications with a reference (B)) via the application layer. The policy control agent A communicates service settings and/or configuration information via this communications stack, as shown (illustrating such communications with a reference (D)) via the policy implementation agent layer and/or the modem firewall layer. The connection manager agent communicates select & control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C)) via the modem driver layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (E)) at the application layer through the modem driver layer with the service monitor agent B as shown (and an access control integrity agent B is also shown), and communications with references (F) at the policy implementation

agent layer and (G) at the modem firewall layer with the service monitor agent A as shown (and an access control integrity agent A is also shown). In some embodiments, the service usage policy verification or tamper prevention embodiments described herein can be applied, in isolation or in combination, in the context of FIG. 31 to provide for embodiments with increasing levels of service usage policy control verification certainty, such as provided with FIGS. 26A-26H, 27A-27P and 28A-28E.

[0341] FIG. 31 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the service processor is a simplified implementation. For example, this approach can be used for applications with less capable device application processors, rapid time to market needs, fewer service usage control needs, and/or other reasons that lead to a need for a lower complexity implementation.

[0342] Referring to FIG. 31, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for the modem layer at the bottom of the device communications stack. The modem driver layer resides above the modem bus layer as shown. In the next higher layer, the policy implementation agent is provided, and the policy implementation agent is also in communication with the agent communication bus 1630 as shown. The next higher layer is shown as the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown. The connection manager communicates select and control as well as modem and access network information via the modem driver as shown. Although FIG. 31 does not depict all of the service usage control verification functions provided by certain embodiments calling for additional service verification or control agents, a high level of service policy implementation verification certainty can be

achieved within the context of the embodiments depicted in FIG. 31 by applying a subset of the service usage policy verification or tamper prevention embodiments described herein. For example, the embodiments depicted in FIG. 31 can be combined with the service controller embodiments that utilize IPDRs to verify service usage is in accordance with the desired service policy. There are also many other service usage control embodiments described herein that can be applied in isolation or in combination to the embodiments depicted in FIG. 31 to provide increasing levels of service usage control verification certainty, as will be apparent to one of ordinary skill in the art in view of FIGS. 26A-26H, 27A-27P and 28A-28E and the various embodiments described herein.

[0343] FIG. 32 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the service processor is a simplified implementation embodiment with device based monitoring and integrity control. For example, FIG. 32 provides for somewhat higher complexity (e.g., relative to the embodiments depicted in FIG. 30) in exchange for the enhanced service monitoring, control or verification that are possible by implement additional agent embodiments, such as the service monitor agent and the access control integrity agent functions.

[0344] Referring to FIG. 32, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point II resides above the modem selection & control layer, which resides above the modem buses for each modem. Measurement point I resides between the policy implementation agent (policy based router/firewall) layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown. The connection manager communicates select and

control as well as modem and access network information via the modem selection and control layer as shown. The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. As similarly described with respect to FIGS. 30 and 31, many of the service usage control verification embodiments described herein can be applied in isolation or in combination in the context of FIG. 32.

[0345] FIG. 33 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. Referring to FIG. 33, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point III resides above the modem selection & control layer, which resides above the respective modem buses for each modem. Measurement point II resides between the policy implementation agent (policy based router/firewall) layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 33.

[0346] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communicates user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or

configuration information via this communications stack, as shown (illustrating such communications with a reference (B)) via the policy implementation agent layer. The connection manager agent communicates select & control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C)) via the modem selection and control layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (D)) at the application layer and (E) at the policy implementation agent layer.

[0347] As shown in FIG. 33, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through III, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. As similarly described with respect to FIGS. 30, 31 and 32, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 33.

[0348] FIG. 34 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the data path processing for the service processor is provided in conjunction with a single modem driver as shown. As shown, the service processor communication stack processing is provided below the standard network communication stack and in combination with a modem driver (e.g., and this approach can be extended to more than one modem).

[0349] Referring to FIG. 34, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point II resides above the modem driver 1 layer.

Measurement point I resides between the policy implementation agent (policy based router/firewall) layer and the modem selection and control layer, for the modem driver 1 stack in this single modem driver embodiment. The transport layer, including TCP, UDP, and other IP resides above the IP queuing and routing layer, which resides above the modem selection and control layer, as shown. The session layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer, resides above the transport layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer.

[0350] As shown in FIG. 34, applications communicate with the device communications stack via the network services API as shown (illustrating such communications with a reference (A)). Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown (illustrating such communications with a reference (B)). The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with policy implementation agent layer of the device communications stack. Also, the service monitor agent performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (C)) at the policy implementation agent layer. Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. As similarly described with respect to FIGS. 30, 31, 32 and 33, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 34.

[0351] FIG. 35 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 35 illustrates a

single modem hardware embodiment as shown. As shown, the service processor network communication stack processing is provided on the modem hardware (e.g., and this approach can be extended to more than one modem). This approach allows for the service processor to be distributed as a standard feature set contained in a modem chipset hardware or software package or modem module hardware or software package, which, for example, can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity, or other benefits.

[0352] Referring to FIG. 35, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. As shown, measurement points I and II and the policy implementation agent reside on the modem 1 (e.g., implemented as hardware and/or software on modem 1). Measurement point I resides above the policy implementation agent (policy based router/firewall) layer, and measurement point II resides below the policy implementation agent layer. The modem selection and control layer resides above the modem drivers layer, as shown. The transport layer, including TCP, UDP, and other IP resides above the IP queuing and routing layer, which resides above the modem selection and control layer, as shown. The session layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer, resides above the transport layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer.

[0353] As shown in FIG. 35, applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown (illustrating such communications with a reference (A)). The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with policy implementation agent layer of the modem 1. Also, the service monitor agent performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information.

An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (B)) at the policy implementation agent layer. As similarly described with respect to FIGS. 30, 31, 32, 33 and 34, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 35.

[0354] FIG. 36 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 36 illustrates a single modem hardware embodiment, in which modem 1 includes a portion of the service processor networking communication stack processing and measurement points II and III and the policy implementation agent, as similarly shown in FIG. 35, and the higher levels of the device communications stack above the modem 1 layer, such as the application service interface layer, are implemented on the device application processor or in the device application processor memory as similarly described above, for example, with respect to FIG. 33, in which a measurement point I is shown between the application service interface agent layer and the network services API layer. For example, this approach allows for the application service interface agent to be provided on the device application processor or memory so that application layer service usage monitoring or control can be implemented. For example, the differences between the embodiments depicted in FIG. 36 and those of FIG. 30 include a simplified implementation and a policy control agent that is entirely implemented on the modem and not partially implemented in the application processor memory.

[0355] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or configuration information via this communications stack, as shown (illustrating such

communications with a reference (B)) via the policy implementation agent layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with reference (C) at the application layer and communications with reference (D) at the policy implementation agent layer). As shown, the service monitor agent B communicates with the application service interface agent and measurement point I, and the service monitor agent A communicates with the policy implementation agent layer and measurement points II and III of the modem 1. As similarly described with respect to FIGS. 30, 31, 32, 33, 34 and 35, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 36.

[0356] FIG. 37 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 37 illustrates a device communications stack as similarly shown in FIG. 36, with the difference being that the service processor subsystem networking communication stack processing is implemented on a hardware function that is separate from the application processor and the modem. For example, this approach provides security advantages with a dedicated hardware system to protect some or all of the service usage control system from tampering. For example, some or all of the service processor can be implemented on a SIM card module. As another example, some or all of the service processor can be encapsulated on a self contained hardware module that can be added to a device without the need to modify the networking communication stack software or hardware.

[0357] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG. 38. For example, the service processor packet processing flow can be performed by the device communications stack, such as described above with respect to FIG. 29. The various embodiments for packet processing flow depicted in FIGS. 38 through 40 are self explanatory to

one of ordinary skill in the art and not all the processing steps and flow sequences are described herein.

[0358] In some embodiments, the burst size, buffer delay, acknowledgement delay and drop rate used in upstream and downstream traffic shaping are optimized with the goal of reducing access network traffic overhead, and excess capacity usage that can result from mismatches in traffic transmission parameters with the access network MAC and PHY or from excess network level packet delivery protocol re-transmissions. In some embodiments, an application interface agent 1693 is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. As shown in FIG. 16, the application interface agent 1693 is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[0359] Referring to FIGS. 38 through 40, in some embodiments, the upstream traffic service policy implementation step corresponds to the traffic shaping step described herein. Referring to FIG. 38, this step is depicted as shown as an alternate exploded view including four upstream sub-steps of apply QoS queue priority, apply traffic shaping rules, network optimized buffer/delay and remove application ID tag. An additional approach shown in FIG. 38 involves two exploded view sub-steps associated with the firewall service policy implementation step and these sub-steps are pass/block packet and pass/redirect packet. For example, the functions performed by these six sub-steps can be depicted in any number of sub-steps, the order of the steps can be appropriately performed in various different orders to provide for upstream traffic shaping within the network communication stack. For example, FIGS. 39 and 40 show the two steps of policy implementation and firewall as one step and the six exploded view sub-steps are included under the same policy implementation step and are performed in a different order than in FIG. 38. It should also be noted that a number of embodiments are possible in which the access control, traffic control or firewall functions are moved to the application service interface layer or another layer.

[0360] Referring now to the downstream portion of FIG. 38, there are two steps again termed traffic service policy implementation and firewall service policy implementation in this

traffic shaping, access control and firewall example. These two packet flow processing steps are depicted as shown in the exploded view as the five sub-steps of tag with flow ID, pass/block packet, apply QoS, apply traffic shaping rules and network optimized buffer, delay, and drop. As with the upstream packet processing flow, the number of sub-steps, the order of sub-steps and the location of the sub-steps in the downstream networking stack processing can be depicted in any number of sub-steps, order and/or location, and various other embodiments will be apparent to one of ordinary skill in the art, including embodiments which locate some or all of the steps in the application service interface layer or other layers as depicted in FIGS. 39 and 40. The details of the packet flow processing design for the downstream can be somewhat more complex in certain embodiments as compared to the upstream processing in two ways. First, as described herein, in some embodiments, the packet tagging that requires application level information can require the initial portion of the packet flow burst to pass through the upstream networking communication stack until the application service interface layer can associate the packet flow with the appropriate information visible at the application level at which time the packet flow tag is communicated to the other service processor agent functions so that they can properly monitor or control the traffic associated with the flow.

[0361] Independently, another complication arises when upper layer reliable communication protocols, such as TCP, are employed in the networking stack in which the downstream transmitting end repeats the packet transmission if the receiving TCP protocol stack does not send a packet receipt acknowledge (ACK) within a certain period of time. If packets are arbitrarily delayed or dropped, then the TCP re-transmission traffic can reduce, completely eliminate or even reverse the network capacity advantage gained by reducing the average traffic speed or other transmission quality measure for one or more service activities. To solve this problem, in some embodiments, the packet traffic control parameters (e.g., downstream delay, drops, burst length, burst frequency and/or burst jitter) are optimized for TCP re-transmission efficiency so that changes in traffic control access bandwidth or speed for one or more service activities are implemented in such a manner that the TCP re-transmission delay at the network transmitting end adapts to be long enough so that wasted packet re-transmission bandwidth is reduced. In addition, and either in combination or in isolation, in some embodiments, the packet traffic control parameters (e.g., downstream delay, drops, burst length, burst frequency and/or

burst jitter) can be adjusted so that the access network downstream MAC and/or PHY efficiencies are optimized.

[0362] Numerous other embodiments for the detailed implementation of packet flow processing in both downstream and upstream will be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, as described herein, the following are provided: (A) traffic shaping is performed in a verifiable manner, (B) traffic shaping is performed in a manner that results in improved network capacity by taking into account to some degree the manner in which the access network PHY layer and/or MAC layer responds to packet parameters (e.g. burst delay, burst drops, burst length, burst frequency and/or burst jitter), (C) traffic shaping is performed in a manner that results in improved network capacity by taking into account how the packet parameters (e.g., burst delay, burst drops, burst length, burst frequency and/or burst jitter) impact layer 3 and higher ACK protocol or other network protocol network capacity efficiencies, (D) packet shaping is performed in a manner that is aware of and optimized for the particular type of communication protocol or packets being sent (e.g., TCP packets can be dropped to slow the application rate of transfer whereas UDP packets are never dropped, because there is no re-transmission), (E) a virtual or literal packet tagging system is used in a verifiable traffic shaping service control system to provide a deeper level of service monitoring and control or to simplify the processing of the packets, and/or (F) starting with these low level packet processing, traffic control or access control building blocks one or more additional layers of higher level policy control can be added on the device or in the network to create service profiles for the service provider network that define complete services, such as ambient services and many other variations of service profile settings that each define a device or user service experience and can be associated with a billing plan. For example, the use of higher layers of service profile control to form more complete service solutions starting with these relatively simple low-level traffic control, access control or firewall processing steps or functions is also described herein.

[0363] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG.

39 (e.g., of a less feature rich device service processor embodiment, such as one similar to that depicted in FIG. 32).

[0364] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG. 40 (e.g., of a mid-featured embodiment of a device service processor, such as one similar to that depicted in FIG. 33).

[0365] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments. Many of these privacy levels are similarly described above, and the table shown in FIG. 41 is not intended to be an exhaustive summary of these privacy levels, but rather is provided as an aid in understanding these privacy levels in accordance with user privacy related embodiments described herein. For example, there are many other parameters that can be associated with privacy filtering, and as will be apparent to one of ordinary skill in the art in view of the various embodiments described herein, the unique feature of user defined or user influenced privacy filtering for service usage, service activity or CRM reports can be implemented with a variety of embodiments that are variations of those described herein.

[0366] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments. Many of these service policy control commands are similarly described above, and the tables shown in FIGS. 42A-J are not intended to be an exhaustive summary of these service policy control commands and do not include summaries of all the embodiments described herein, but rather are provided as a summary aid in understanding these service policy control commands in accordance with various embodiments described herein.

[0367] In some embodiments, QoS is employed for devices with a service processor 115. For example, QoS can be employed in a crowded hot spot where the service processor 115 profile has been changed from WWAN to WLAN, but the WLAN is backed up as too many users are trying to use it. The service processor 115 can have a hierarchical access to the hotspot

at that point; or the service processor 115 that pays less can be throttled while those that pay more are opened up; or the service processor 115 can initiate a policy that slows down transmissions to improve trunking efficiency.

[0368] FIGS. 43A through 43B are flow diagrams illustrating a flow diagram for a service processor authorization sequence as shown in FIG. 43A and a flow diagram for a service controller authorization sequence as shown in FIG. 43B in accordance with some embodiments.

[0369] Referring to FIG. 43A, at 4302, the device is in an offline state. At 4304, the service processor (e.g., service processor 115) of the device collects device service processor credentials and access control integrity information. At 4306, the service processor of the device selects a best network. At 4308, the device connects to an access network. At 4310, the service processor of the device sends an authorization request to the service controller (e.g., service controller 122) and also sends the credentials and access control integrity information. At 4312, the service processor determines whether an integrity error has occurred. If so, then the service processor performs integrity error handling at 4314. Otherwise, the service processor determines whether the device is activated and/or authorized for network access at 4316. If not, then the service processor performs a device activation sequence at 4318. At 4320, the service processor performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4322, the device is in an online state.

[0370] Referring to FIG. 43B, at 4332, device control is in an offline state. At 4334, the service controller (e.g., service controller 122) receives a device authorization request, verifies device service plan standing, verifies device access control integrity standing, verifies device access control integrity information, verifies service processor heartbeat, and performs various additional service processor integrity checks (e.g., as similarly described herein). At 4336, the service controller determines whether the device integrity checks have all passed. If not, then the service controller sends an integrity error to the service processor (e.g., service processor 115) at 4338. At 4340, the service controller performs integrity error handling. Otherwise (the device integrity checks have all passed), the service controller determines whether the device is

activated at 4342. If not, then the service controller sends an activation message to the service processor at 4344. At 4346, the service controller performs a service activation sequence. Otherwise (the device is activated), the service controller sends an authorization at 4348. At 4350, the service controller performs the following: updates critical software on the service processor, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, sends stored CRM and billing information. At 4352, the service controller is in a device online state.

[0371] FIGS. 44A through 44B are flow diagrams illustrating a flow diagram for a service processor activation sequence as shown in FIG. 44A and a flow diagram for a service controller activation sequence as shown in FIG. 44B in accordance with some embodiments.

[0372] Referring to FIG. 44A, at 4402, a service processor activation sequence is initiated. At 4404, the service processor (e.g., service processor 115) of the device displays an activation site (e.g., HTTP site, WAP site or portal) to the user for the user's service activation choice. At 4406, the user selects service plan, billing information and CRM information. At 4408, the service processor sends an activation request and user billing and CRM information to, for example, the service controller. At 4410, the service processor determines whether there is an integrity error. If so, then the service processor performs integrity error handling at 4412. Otherwise, the service processor determines whether there has been a selection input error at 4414. If so, the service processor displays the selection input error to the user at 4416 and returns to the activation site/portal at 4404. Otherwise, the service processor identifies the activated service plan at 4418. At 4420, the service processor performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4422, the device is in an online and activated state.

[0373] Referring to FIG. 44B, at 4432, a service controller activation sequence is initiated. At 4434, the service controller (e.g., service controller 122) receives an activation request, including user billing and CRM information, and sends such to central billing. At 4436,

the service controller receives a response from central billing. At 4438, the service controller verifies the integrity of the service processor. If an integrity error is detected, then an integrity error is sent at 4440. At 4442, the service controller performs integrity error handling. At 4444, the service controller determines whether the service plan has been activated. If not, then the service controller sends a selection input error to the device at 4446 and returns to 4432. Otherwise (device has been activated), the service controller sends the service plan activation information to the device at 4448. At 4450, the service controller performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4452, the service controller is in a device online and activated state.

[0374] FIGS. 45A through 45B are flow diagrams illustrating a flow diagram for a service processor access control sequence as shown in FIG. 45A and a flow diagram for a service controller access control sequence as shown in FIG. 45B in accordance with some embodiments.

[0375] Referring to FIG. 45A, at 4502, the device is in an online state. At 4504, the service processor (e.g., service processor 115) of the device processes any new heartbeat messages received from the service controller (e.g., service controller 122). At 4506, the service processor updates software if necessary, updates service policy and control settings if necessary, synchronizes service counters, updates service cost data if necessary, and updates CRM rules if necessary. At 4508, the service processor performs access control integrity checks. At 4510, the service processor determines whether there are any access control integrity errors. If so, then the service processor performs integrity error handling at 4512. Otherwise, the service processor updates user service UI gauges, provides notification if necessary, and accepts input if available at 4514. At 4516, the service processor sends new service processor heartbeat messages to the heartbeat message queue. At 4518, the service processor processes any pending billing transactions. At 4520, the service processor determines if a heartbeat transmission is due, and if not, returns to 4504 for processing any received heartbeat messages. If so, at 4522, the service processor sends the new service processor heartbeat message to the service controller.

[0376] Referring to FIG. 45B, at 4532, the device is in an online state. At 4534, the service controller (e.g., service controller 122) processes any new heartbeat messages received from the service processor. At 4536, the service controller performs access control integrity checks. At 4538, the service controller determines whether there are any access control integrity errors. If so, then the service controller performs integrity error handling at 4540. At 4542, the service controller updates the billing database, updates the CRM information, synchronizes service counters, updates cost database if needed, and synchronizes CRM rules if necessary. At 4544, the service controller processes any pending billing transactions. At 4546, the service controller sends new service processor heartbeat messages to the heartbeat message queue. At 4548, the service controller determines if a heartbeat transmission is due, and if not, returns to 4534 for processing any received heartbeat messages. If so, at 4550, the service controller sends new service processor heartbeat message to the service processor.

Open Content Distribution and Transaction System

[0377] Referring now to FIGS. 46 and 47A-47B, in another set of embodiments an open, decentralized, device based system for enabling central billing for third party electronic commerce transactions for mobile commerce is provided as shown. For example, in these embodiments, device information can be embedded in HTTP, WAP or other portal browser/network header request information that indicates a central billing option is available to a compatible third party transaction server, as further described below with respect to FIGS. 46 and 47A-47B.

[0378] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments. As shown, a service processor 4615 of the device 100 (e.g., any mobile device capable of storing and executing the service processor 4615) includes access control integrity agent 1694, billing agent 1695, agent communication bus 1630, user interface 1697, policy control agent 1692, service monitor agent 1696, application interface agent 1693, policy implementation agent 1690, and modem router and firewall 1655, as similarly described herein with respect to various other service processor embodiments. In some embodiments, an application 4604 (e.g., an HTML/WAP web browser) and a mobile payment agent 4699 are also included in the device, such as part of the service

processor 4615 as shown. In some embodiments, the application 4604 is not integrated as part of the service processor 4615, but is executing and/or stored on the device. In some embodiments, the mobile payment agent 4699 includes billing agent 1695, user interface 1697 and/or application interface agent 1693, and/or various other functional components/agents. As shown, the service processor 4615 is in communication with a carrier access network 4610, which is in network communication with the Internet 120.

[0379] In some embodiments, device information can be embedded in HTTP, WAP or other portal browser/network header request information that indicates a central billing option is available to a compatible third party transaction server, such as the open content transaction partner site(s) 134. For example, the compatible transaction server can then send a signed confirmation request over a pre-assigned control socket channel to the billing agent 1695 with the billing agent 1695 confirming the signed confirmation request by either performing the signature check locally based on a stored and synchronized list of approved transaction servers or by passing the signed request onto a billing server 4630 for confirmation. Optionally, in another example, a triangle confirmation can be set up in which the billing server 4630 can confirm the transaction set up with the transaction server 134 or the transaction server 134 can confirm the transaction set up with the billing server 4630. Once the device confirms the compatible and approved status of the transaction server 134, the device/transaction server pair can then optionally further exchange keys for the remainder of the transaction for enhanced security. In another example, the transaction server 134 can also redirect the user browsing experience to one tailored to one or more of device type, service provider, device manufacturer or user. When the user selects a transaction, the transaction server sends the billing agent 1695 a transaction bill that describes the transaction and the amount. The billing agent 1695 can optionally confirm that the user account has sufficient credit limit to make the purchase by either confirming the stored credit limit on the device or querying the billing server 4630. The billing agent 1695 then invokes the device UI 1697 to display the transaction description and amount and request user approval for the billing to be conducted through the central billing option. User approval can be acquired, for example, by a simple click operation or require a secure password, key and/or biometric response from the user. Upon user approval, the billing agent 1695 generates a billing approval and sends it to the transaction server 134, the transaction server 134 completes the transaction and then sends a bill to the billing agent 1695. The billing agent 1695 optionally

sends a confirmation to the transaction server 134 and sends the bill to the billing server 4630. Again, optionally a triangle confirmation can be formed by the billing server sending a confirmation to the transaction server 134, or the transaction server 134 can send the bill to the billing server 4630. In some embodiments, the billing server 4630 can also communicate such billed transactions to a central provider billing system 4623 via the carrier access network 4610. Also, in some embodiments, an alternate location billing server 4632 is in communication via the Internet 120, and an alternate location central provider billing system 4625 is also in communication via the Internet 120.

[0380] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments. Referring to FIG. 47A, the device application 4604 browses (e.g., based on the user submitting a browse request using a browser application) to transaction server 134 (e.g., a transaction web server, such as the open content transaction partner site 134). The transaction server 134 provides an offer to the device application 4604. The device application 4604 selects a purchase (e.g., based on the user's selection input). In response, the transaction server 134 seeks an API connection with the device mobile payment agent 4699, which then confirms the API connection. The transaction server 134 requests user purchase confirmation (mediated by the device mobile agent 4699 as shown), and the purchase is confirmed by the device application 4604 (e.g., based on the user's acknowledgement as similarly described above with respect to FIG. 46). The transaction server 134 then transmits a purchase receipt, and the device application 4604 confirms the receipt. The transaction server 134 then transmits the purchase bill to the device mobile payment agent 4699, which then sends the purchase bill to the device billing server (e.g., billing server 4630). The transaction server also optionally sends a confirmation of the purchase bill to the device billing server for a triangle confirmation, as similarly described above with respect to FIG. 46. The device billing server sends a copy of the purchase bill to the central provider billing system (e.g., central provider billing system 4623).

[0381] Referring now to FIG. 47B, the device application 4604 browses (e.g., based on the user submitting a browse request using a browser application) to transaction server 134 (e.g., a transaction web server, such as the open content transaction partner site 134), in which the browse request includes device ID information, such as similarly described above with respect to

FIG. 46. The transaction server 134 establishes API contact with the device mobile agent 4699, which then confirms contact and good standing for transactional purchases from the device. The transaction server 134 provides an offer to the device application 4604. The device application 4604 selects a purchase (e.g., based on the user's selection input). The transaction server 134 notifies the device mobile payment agent 4699 of the purchase description and amount, and the device mobile payment agent 4699 then requests user purchase confirmation. The purchase is confirmed by the device application 4604 (e.g., based on the user's acknowledgement as similarly described above with respect to FIG. 46), and the device mobile payment agent 4699 then transmits a purchase confirmation to the transaction server 134. The transaction server 134 then transmits a purchase receipt, and the device application 4604 confirms the receipt. The transaction server 134 then transmits the purchase bill to the device mobile payment agent 4699, which then sends the purchase bill to the device billing server (e.g., billing server 4630). The transaction server also optionally sends a confirmation of the purchase bill to the device billing server for a triangle confirmation, as similarly described above with respect to FIG. 46. The device billing server sends the purchase bill to the central provider billing system (e.g., central provider billing system 4623). In some embodiments, the communications described above with respect to FIGS. 47A-47B with the billing server and the central provider billing system are with the alternate location billing server 4632 and/or alternate location central provider billing system 4625 via the Internet 120. Similarly, in some embodiments, the transaction servers 134 are connected to the Internet 120.

[0382] Accordingly, these transaction billing embodiments do not require centralized content storage or content and transaction exchange infrastructure. For example, the transactions can be conducted over the Internet, and the user experience and content can be tailored versions of the transaction server/content provider's normal experience and content. This approach provides for a much wider array of content and transaction partners with minimal or no need to accommodate proprietary specialized systems. Moreover, the compatibility between the device billing agent transaction system and the transaction provider server is easily established, for example, by writing specifications for the header information transmitted by the device and for the secure handshake and signed message transactions that take place between the device billing agent, the transaction server and optionally the transaction server and the billing server. Once a transaction partner shows compatibility test results and concludes a business relationship with

the service provider, the service provider can place the transaction partner on the compatible and approved list and exchange security keys and/or certificates. If a common user experience is desired by the service provider across multiple transaction partners, then the experience specifications for the browser redirects can also be specified in the compatibility specification and tested before the transaction partner gains approval.

Design and Testing for Service Control

[0383] FIG. 48 illustrates a network architecture including a service controller device control system and a service controller analysis and management system in accordance with some embodiments. As described herein, the RAN gateway 410 generally represents the functionality of the various specific RAN gateway functional elements shown and/or discussed herein. For example, these RAN gateway 410 functional elements represent the gateways used to aggregate the radio access network traffic, control, charging and roaming functions and/or other functions and are shown and/or discussed herein using other terminology specific to certain industry standards, including SGSN gateway 410 and gateways 508, 512, 608, 612, 708 and 712. Although the same reference numerals are used for SGSN gateway 410 and RAN gateway 410, it will be appreciated that the RAN gateway 410 represents any or all of the RAN gateway functional elements 410, 508, 512, 608, 612, 708, 712 or any other similar industry equipment or functions depending on the embodiment. Similarly, transport gateway 420 represents the next higher level of gateway aggregation for the transport layer that is used in many networks, and this term transport gateway 420 can be interchanged with any or all of the gateways 420, 520, 620, 720 or any other similar industry equipment or functions depending on the embodiment. Those of ordinary skill in the art will appreciate which gateway description applies to a respective embodiment in which the terms RAN gateway 410, gateway 410, transport gateway 420 or gateway 420 are referenced herein.

[0384] While the embodiments described below with respect to FIGS. 48 through 63 are depicted in the context of a conventional multi-tier access network, one of ordinary skill in the art will appreciate that such embodiments can also be generalized to other network topologies including the various flattened network topologies described herein. As shown, the service controller is divided into two main functions (e.g., as compared with the embodiments of service

controller 122 depicted in FIG. 16): (1) a service controller device control system 4825 and (2) a service controller design, policy analysis, definition, test, publishing system 4835. The service controller device control system 4825 performs the device service control channel functions as previously described herein with respect to various embodiments.

[0385] The service controller design, policy analysis, definition, test, publishing system 4835 separates out the service analysis, control policy design and publishing from the device service control channel functions. The service controller design, policy analysis, definition, test, publishing system 4835 performs a variety of functions as described below. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service usage statistical analysis, notification policy or procedure response analysis and/or billing policy or procedure response analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 detects, singles out and reports device service usage, notification responses or billing behavior that is outside of expected limits but may or may not be violating policy. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service cost and profitability analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides user service control policy, notification policy or billing policy statistical satisfaction analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides statistical take rate analysis for transaction offers and billing offers for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service.

[0386] In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service control policy definition work screens and “dry-lab” (pre-beta) testing against usage database for single devices, groups of devices, types of

devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service control policy, notification policy and/or billing policy beta testing (e.g., using beta test server 1658) in which the beta test profile is published to a subset of users or devices. In some embodiments, beta devices/users may or may not know that the service policy is being tested with them. In some embodiments, if they do know, then beta test apparatus includes offering system that provides user options to accept beta test and provide feedback in exchange for an offer (e.g., show them an offer page that comes up with their existing subscription service or ambient service – offer a free trial, a discount to something and/or reward zone points (or other incentives/rewards) if they accept the trial). In some embodiments, a beta test workstation (e.g., in communication with the beta test server 1658, such as VSP remote workstation 4920 as shown in FIG. 49) allows the beta test manager to define one or more beta test service policy, notification policy and/or billing policy control profiles. In some embodiments, the beta test workstation publishes each profile to specific individual (single) devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the beta test workstation allows the beta test manager to analyze usage statistics, notification response statistics and/or billing/transaction offer response statistics for devices, users, groups of devices or groups of users and compare actual real-time usage versus beta test usage goals. In some embodiments, the beta test workstation allows the beta test manager to fine tune service, notification and/or billing/transaction policies and re-publish to observe changes to actual service usage until the service policy and/or notification control policies achieve the desired result. In some embodiments, the beta test workstation also allows the beta test manager to collect direct user feedback to a set of pre-designed user satisfaction or other questions regarding service usage. For example, questions can be presented through a pre-designed beta test portal or through a series of brief pop-ups that come up when the user initiates a particular action or at a particular time. In some embodiments, the beta test workstation also collects details of service and device usage (e.g., CRM data) that the beta test users have approved for collection. In some embodiments, the beta test workstation can decompose this data to determine if the users are using the service in the manner intended by the beta test goals. In some embodiments, the beta test workstation also allows for publishing multiple variants of the service and/or notification

policy control settings and compare the service usage for each group with convenient screens with information displays (e.g., statistical usage versus time of day, usage of particular activities, billing activity, device discovery activity, user response to notification message and options, user satisfaction with a particular notification policy or billing policy or traffic control policy). In some embodiments, the screens can be designed by the beta test manager.

[0387] In some embodiments, once a service is completely tested and approved for production publication, the service download control server 1660 has a workstation screen that allows the service manager to specify which group of devices are to receive the new service policy configuration. In some embodiments, the service download control server 1660 allows the service manager to define specific individual (single) devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service.

[0388] In some embodiments, a service (e.g., a newly created or new version of an existing service) is tested and/or enhanced using a new service testing model. For example, a new service (or a new version of an existing service) is loaded onto a server for testing, the new service is (optionally) tested against existing device usage statistics, a new service control definition (e.g., implemented as service processor 115 for publishing to devices 100 and a corresponding new service controller 122 for the service provider, such as a central provider or an MVNO partner, and, for example, the new service processor and service controller can be implemented using the below described SDK) for the new service is developed and possibly adjusted based on the testing against existing device usage statistics, the new service control definition is then published to beta devices (e.g., various devices 100 used for beta testing the new service), which then use the new service, service usage statistics and/or user feedback statistics are then collected (e.g., to ensure that the service is functioning properly and so that the service control definition can be tuned to ensure adequate service, user experience and for service pricing/profitability purposes), the service/service control definition is then fine tuned based on the service usage/user feedback statistics. Upon completion of the above testing and refinement of the service/service control definition, the service control definition can be published to specified groups of devices for using the new service. In some embodiments, this service control testing model for groups of devices and service partners is provided by a virtual

MVNO or VSP. For example, this allows for new services to be more efficiently and more effectively developed, tested and proliferated.

[0389] In some embodiments, service history IPDRs come from within a networking component connected to the central provider core network 110 as depicted by (e.g., real-time) service usage 118 (which as discussed elsewhere is a general purpose descriptor for a function located in one or more of the networking equipment boxes). In some embodiments, service history IPDRs are collected/aggregated (in part) from the central billing system 123. In some embodiments, service history IPDRs are collected/aggregated (in part) from the transport gateways 420. In some embodiments, service history IPDRs are collected/aggregated (in part) from the RAN gateways 410. In some embodiments, service history IPDRs are collected/aggregated (in part) from the base station(s) 125 or a networking component co-located with the base station(s) 125, a networking component in the transport network 415, a networking component in the core network 110 or from another source.

Virtual Service Provider for Service Control

[0390] In some embodiments, virtual service provider (VSP) capabilities include making available to a third party service partner one or more of the following: (1) device group definition, control and security, (2) provisioning definition and execution, (3) ATS activation owner, (4) service profile definitions, (5) activation and ambient service definition, (6) billing rules definition, (7) billing process and branding controls, (8) bill by account settings, (9) service usage analysis capabilities by device, sub-group or group, (10) beta test publishing capabilities by device, sub-group or group, and (11) production publishing, fine tuning and re-publishing.

[0391] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments. As shown, the service controller design, policy analysis, definition, test, publishing system 4835 is configured so that multiple “service group owners” (e.g., the service provider for certain smart phones) or “device group owners” (e.g., eReader devices for the eReader service provider(s)) or “user group owners” (e.g., IT for Company X for their employees’ corporate mobile devices), collectively referred to as the “Virtual Service Provider” (VSP), are serviced with the same service controller infrastructure and the same (or substantially similar) service processor design

from virtual service provider workstation server 4910 and/or virtual service provider remote workstation(s) 4920. As shown, the virtual service provider remote workstation(s) 4920 communicates with the virtual service provider workstation server 4910 via VPN, leased line or secure Internet connections. The dashed lines shown in FIG. 49 are depicted to represent that, in some embodiments, the virtual service provider workstation server 4910 is networked with the service controller device control system 4825 and/or, in some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835. Based on the discussion herein, it will be apparent to one of ordinary skill in the art that the VSP workstation server 4910 can also be networked in various embodiments with billing system 123, AAA server 121, gateways 410 or 420, or other network components to perform, for example, various network provisioning and activation related functions discussed herein for the device group assigned to one or more VSPs, or for other reasons as will be apparent to a given VSP embodiment.

[0392] In some embodiments, the service controller functionality is partitioned for a VSP by setting up one or more secure workstations, secure portals, secure websites, secure remote software terminals and/or other similar techniques to allow the service managers who work for the VSP to analyze, fine tune, control or define the services they decide to publish to one or more groups of devices or groups of users that the VSP “owns.” In some embodiments, the VSP “owns” such groups by virtue of a relationship with the central provider in which the VSP is responsible for the service design and profitability. In some embodiments, the central provider receives payment from the VSP for wholesale access services. In some embodiments, the VSP workstations 4910 and 4920 only have access to the service analysis, design, beta testing and publishing functions for the devices or users “owned” by the VSP. In some embodiments, the user or device base serviced by the central provider network is securely partitioned into those owned by the central provider, those owned by the VSP, and those owned by any other VSPs.

[0393] In some embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using device based service control techniques as described herein. In some embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using device assisted and network based service control techniques as described herein. In some

embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using network based service control techniques (e.g., DPI techniques) as described herein.

[0394] For example, this approach is particularly well suited for “open developer programs” offered by the central providers in which the central provider brings in VSPs who offer special value in the devices or service plans, and using this approach, neither the central provider nor the VSP needs to do as much work as would be required to set up a conventional MVNO or MVNE system, which often requires some degree of customization in the network solution, the billing solution or the device solution for each new device application and/or service application that is developed and deployed. In some embodiments, the service customization is simplified by implementing custom policy settings on the service processor and service controller, and the custom device is quickly brought onto the network using the SDK and test/certification process. In some embodiments, the VSP functionality is also offered by an entity other than the central provider. For example, an MVNE entity can develop a wholesale relationship with one or more carriers, use the service controller to create the VSP capabilities, and then offer VSP services for one network or for a group of networks. In some embodiments, the service customization is simplified by implementing custom policy settings through the VSP embodiments on the network equipment, including, in some embodiments, service aware or DPI based network equipment that has a relatively deep level of service activity control capability. For example, using the embodiments described herein, and possibly also including some of the activation and provisioning embodiments, it is possible to efficiently design and implement custom ambient service plans that are different for different types of devices, different OEMs, different VSPs, different distributors, or different user groups all using the same general infrastructure, whether the service control policy implementation is accomplished primarily (or exclusively) with networking equipment (network) based service control, primarily (or exclusively) with device based service control or with a combination of both (e.g., hybrid device and network based service control).

[0395] As discussed herein, various VSP embodiments for performing one or more of analyzing traffic usage and defining, managing service profiles or plans, dry lab testing service profiles or plans, beta testing service profiles or plans, fine tuning service profiles or plans, publishing service profiles or plans, or other policy related settings can involve programming

settings in the network equipment and/or programming settings or software on the device. For example, as discussed herein, the service processor settings are controlled by the service controller, which can be partitioned to allow groups of devices to be controlled. As another example, equipment in the network involved with network based service control, such as DPI based gateways, routers or switches, can similarly be programmed to utilize various VSP embodiments to implement that portion of the service profile (or service activity usage control) that is controlled by network level functions, and it will be appreciated that substantially all or all of the service activity control for certain embodiments can be accomplished with the network functions instead of the device. Continuing this example, just as the device service processor settings control functions of the service processor can have a group of devices that are partitioned off and placed under the control of a VSP, various VSP control embodiments can partition off a group of devices that have service usage activity controlled by the networking equipment, including, in some embodiments, sophisticated service aware DPI based service control equipment, to achieve similar objectives. It will be appreciated that the discussion herein regarding service controller design, policy analysis, test, publishing 4835, and the discussion regarding device group, user group and other VSP related embodiments, should be understood as applicable to various embodiments described in view of device based services control, control assistance and/or monitoring, or network based services control, control assistance and/or monitoring, or a combination of device based services control, control assistance and/or monitoring and network based services control, control assistance and/or monitoring. The various embodiments described herein related to service activation and provisioning also make apparent how the programming of network equipment service control, service control assistance and/or monitoring can be implemented prior to and following activation of the device. It will also be appreciated that the VSP capabilities described herein can also be applied to those devices that have services controlled by, provided by and/or billed by the central provider, so these techniques can be applied to central provider service embodiments, MVNO embodiments and other embodiments.

Open Development System for Access Services – SDK

[0396] In some embodiments, an SDK is provided that allows developers, such as device manufacturers, service providers, MVNO, MVNE and/or VSPs, to develop various service

processors (e.g., different versions of the service processor 115) for various devices (e.g., various types of devices 100) and corresponding service controllers (e.g., different versions of the service controller 122) for various types of services and network environments. For example, a device manufacturer can use the SDK to develop a new service processor for their new device (e.g., mobile phone, PDA, eBook reader, portable music device, computer, laptop, netbook, or any other network accessible device). The device manufacturer can also preload/preinstall their new service processor on their new devices. In this example, users of the new device would then be able to utilize the new device to access network based services using the new service processor, which communicates with the deployed new service controller, as similarly discussed herein in various embodiments. For example, the device can be preinstalled with the new service processor to provide ambient services, as similarly discussed herein in various embodiments. For example, the SDK can allow for substantially similar service processors to be installed on similar and/or different devices thereby minimizing any unnecessary differences between service processor elements for device assisted services. In some embodiments, for ambient services for a group of devices, or devices associated with a certain service provider, a set of numbers (e.g., dummy numbers) can be assigned for use for attempting access via the access network using a new device that is not yet otherwise subscribed for service. In some embodiments, the set of (dummy) numbers used for ambient access by the device can also be used for associate of the device with a service provider or a type of device (e.g., eReader or some other type of network accessible device), and upon activation, the service provider assigns a real number for the activated device (e.g., which can be provided at the time of manufacture of the device, point of sale of the device, or after the point of sale of the device, such as upon activation of the device). For example, ambient access of the device can use the device ID, SIM ID, assigned phone (real or dummy) number, and/or other information associated with the device for assigning appropriate service control and service policy/profile for the device.

[0397] In some embodiments, the service processor 115 is distributed as an SDK to any device that the central provider or the VSP desires to offer services with so that the service processor 115 can be efficiently designed or adapted by the device OEM, ODM or manufacturer for operation on the service network. In some embodiments, the SDK includes either a complete set of service processor 115 agent software designed for and/or tested for the OS (Operating System) and processor set being used on the device, or a mature reference design for the OS and

processor set being used on the device, or a less mature reference design (potentially for the same OS and/or processor set or a different OS and/or processor set being used on the device) that the OEM (Original Equipment Manufacturer) ports to the desired OS or processor set, or a basic set of example software programs that the OEM or ODM (Original Design Manufacturer) can use to develop software compatible with the service, or a set of specifications and descriptions (possibly forming an interoperability standard) of how to design the software to be compatible with the service. In some embodiments, the SDK includes a set of OEM lab test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the SDK includes a set of network certification test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the certification procedures are approved for testing by the OEM, the central provider, the VSP and/or a trusted third party. For example, the central provider is typically in control of the SDK and the test procedures, but others can be in control. In some embodiments, the test procedures are at least in part common across multiple central provider networks. In some embodiments, the SDK concept is extended to include one or more modem modules where one or more of the SDK embodiments described above is combined with a standard reference design or a standard hardware sales package for one or more modems so that the entire package forms a turn-key product that allows a device manufacturer, central provider, VSP or other entity bring new devices or device applications onto the central provider network possibly in combination with other networks in a manner that requires less engineering time and resources and less network certification time and resources than would be required in some designs that do not use this standard SDK plus module approach. For example, the standard SDK plus module product embodiments can be pre-certified and tested with one or more central providers to further reduce development time and expense. The standard SDK plus module embodiments can also use a multi-mode modem (e.g., modems based on a multimode CDMA, EVDO, UMTS, HSPA chipset as in the Gobi global multimode chipset product or modems based on other recently announced LTE plus HSPA chipsets, WiMax plus Wi-Fi chipsets or LTE plus EVDO chipsets) and a multi-mode connection manager agent so that the same SDK plus modem embodiment may satisfy a wide range of applications for many service providers around the world.

[0398] In some embodiments, at the time of manufacture, the device is associated with an MVNO. For example, the MVNO can provide an ambient service that provides a service provider clearing house, in which the device can access a network in ambient access mode (e.g., a wholesale MVNO connection through the access network) for purposes of selecting a service provider (e.g., a VSP, MVNO or carrier). Based on the service provider selection, the device credentials and/or service processor are reprogrammed and/or new software is downloaded/installed to activate the device with the selected service provider, as described herein for provisioning the device and the account on that service provider network (e.g., the ATS can track such activation, for example, for revenue sharing purposes, as an activation incentive fee).

[0399] In some embodiments ATS is implemented entirely in the network as described below. At the time of manufacture or at sometime during device distribution, the device master agent programs a unique credential in the device that cannot be re-programmed or removed (or is difficult to re-program or remove) and that can be recognized and recorded by the network at the time of activation or at some other time. In this manner, even if other, possibly primary, device credentials are reprogrammed or removed, there will still be a credential that is associated with the device master agent. The ATS process can then be implemented by using a database search function to scan through the database of activated devices to form a list of devices that have been activated for the purpose of master agent reconciliation. Example credentials that can suffice are MEID, hardware MAC address, and/or serial number, that are picked up and recorded by the service provider or other service entity at time of activation or before or after activation.

Interface Server Overlay for Billing/IPDR Feed Mediation

[0400] FIG. 50 illustrates a network architecture including a billing to service controller interface for accommodating minimum changes in existing central billing, AAA and/or other network components in accordance with some embodiments. As shown, the central billing system 123 includes a mediation, customer service and billing databases, historical usage, billing systems component 5010 and a billing to service controller interface component 5020. For example, the billing to service controller interface component 5020 allows for the central billing

system 123 to efficiently communicate with the service controller (e.g., service controller device control system 4825).

[0401] In some embodiments, an interface server (e.g., the billing databases, historical usage, billing systems component 5010 and/or the billing to service controller interface component 5020) is provided that reads the IPDRs, service profile and/or service plan information stored in the billing and/or service record database(s). In some embodiments, the interface server performs these functions in a manner that is compatible with communication formats of the billing and/or service record database(s) so that little or no changes are required in the configuration, communication formats or software of the existing central billing, AAA and/or other network components. In some embodiments, the interface server (e.g., including the billing databases, historical usage, billing systems component 5010 and the billing to service controller interface component 5020) is co-located with the central billing system components as shown, or in other embodiments, the interface server is located elsewhere. For example, the interface server can be located close to or within the components that comprise the service controller or anywhere else in the network.

[0402] In some embodiments, the interface server performs certain communication protocol translation or data format translation required to interface the information stored in the billing and/or service record database(s) to the service controller functions so that the central billing system 123 and other existing components in the network do not need to change much (if at all) to enable the service controller and service processor to implement device based/assisted service control. In some embodiments, the central billing system 123 or other network components are not required to be aware of the service control functions being implemented by the service controller or service processor, because the interface server acquires the network based information needed by the service controller and/or service processor while requiring little or no specialized awareness, communication, data formatting, user interfacing, service profile processing or service plan processing on the part of existing billing, database or networking components. In this type of overlay approach, various embodiments described herein can be used to quickly upgrade the capabilities of existing networks for new devices while minimizing the required changes to the existing network that supports legacy devices.

[0403] For example, a new ambient service plan can be implemented within the central billing system 123 that is associated with a zero or low cost billing plan and a usage limit (e.g., ambient service) that may be difficult or impossible to support in a manner that would result in high user satisfaction and a high level of control for service cost and service policy definition. Even if the central billing system 123 is not highly involved in the process, the zero or low cost plan can be implemented in a manner that results in high user satisfaction and a cost controlled service by using the service controller and/or service processor and the interface server to implement the ambient services access control, service usage control, user interface, service usage notification, transaction billing or bill by account functionality. For example, this approach can be implemented by reading the service plan and/or service policy settings for a device in the central billing database using the interface server, looking up the corresponding service policy, user notification policy, transaction billing policy and bill by account policy associated with the particular service profile or service plan, and then implementing the policies with the assistance of the service controller and/or service processor. Similarly, in another definition, multiple tiers of service control and user notification policies can be added to any number of new service profiles or service plans that would not otherwise be supported with the central billing system 123 and other network components, all with minimal or no modifications to the pre-existing network and billing system.

[0404] Another embodiment calls for receiving a standard IPDR feed from central billing 123 or another network component just like an MVNO would. For example, the interface server function can be located in the central billing system, service processor or elsewhere in the network. This provides the IPDR records for service usage policy verification and service usage notification synchronization with little or no need to modify existing billing or network apparatus.

[0405] In some embodiments, duplicate the IPDRs are sent from the network equipment to the billing system and/or network management system that are currently used for generating service billing or are used for device management or network management. In some embodiments, duplicate records are filtered to send only those records for devices controlled by the service controller and/or service processor. For example, this approach can provide for the

same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system.

[0406] In some embodiments, a bill-by-account billing offset is provided using the interface server. For example, bill-by-account billing offset information is informed to the billing system through an existing data feed and by updating the billing database using the interface server. In some embodiments, transaction billing is provided using the interface server. For example, transaction billing log information is provided to the billing system through an existing data feed and by updating the billing database using the interface server.

[0407] In some embodiments, existing/new service plan choice screens are displayed to the user, a user choice or decision/input is confirmed for a selected service plan, and then the service is implemented upon confirmation of the billing system update for the new service plan. In some embodiments, the service is implemented upon the user selection of a new service plan and then retracted if not confirmed as updated by the billing system within a certain period of time. In some embodiments, the new service plan information is updated in the billing system through an existing data feed or by updating the database using the interface server.

Integrated Service Control

[0408] FIG. 51 illustrates a network architecture for locating service controller device control functions with AAA and network service usage functions in accordance with some embodiments. As shown, an integrated device service control, AAA, device usage monitoring system 5110 is provided that integrates service controller functions (e.g., service controller device control system functions 4825 of FIG. 48) with access network AAA server 121 functions and network (e.g., real-time) service usage 118 functions.

[0409] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments. As shown, the service controller device control system 4825 is located in the access transport network 415, or in some embodiments, in the 4G/3G/2G RAN gateways 410 (as indicated by the dashed line with the arrow), or alternatively, in the 4G/3G/2G transport gateways 420 (as indicated by the dashed line with the arrow).

[0410] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments. As shown, the service controller device control system 4825 is located in the radio access network 405, or in some embodiments, in the 4G/3G base station(s) 125 (as indicated by the dashed line with the arrow), or alternatively, in the 3G/2G base stations 125 (as indicated by the dashed line with the arrow).

Ambient Services

[0411] In some embodiments, improved and simplified processes for provisioning a device or user for service on a central provider network, an MVNO network or a virtual service provider (VSP) on the central provider network are provided. In some embodiments, provisioning includes one or more of the following: a process or result of assigning, programming, storing or embedding into the device and/or network a set of credentials, or otherwise providing the credentials to the user; the credentials being at least in part carried on the device or with the user; and/or at least a portion of or a counterpart to the credentials being stored or recognized by the network so that the various network elements responsible for admitting the device access to the appropriate service activities do so once the device or user service is active.

[0412] As an example, as discussed herein, the credentials can include one or more of the following: phone number, device identification number, MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version, device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar

identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider, OEM, master agent (service distributor), VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user.

[0413] In some embodiments, provisioning includes assigning, programming or embedding into the device and/or network the information to define the level of service activity, referred to as a service profile, that the device is authorized to receive. In some embodiments, provisioning also includes establishing the device settings and/or network settings to define an ambient activation experience in which the device user receives a set of services after (e.g., within a short period of time after) purchasing or otherwise obtaining or installing the device whether the device has or has not been registered and activated with the device user or device owner.

[0414] In some embodiments, the ambient experience is the user experience that is available at the time the device is sold in the event the user has not yet signed up for a service plan. For example, the ambient experience is defined by an ambient service profile, an ambient service plan and/or the other service usage activity control policies in effect in the network, on the device, or a combination of both. For example, if the device service processor is used in large part to define the ambient service profile, then the initial provisioning and activation settings in the service processor, and possibly the service controller, can define the user service upgrade offering choices, network destination access control possibilities, traffic control policies, mobile commerce transaction capabilities (e.g., which transaction websites, WAP sites or portals the user can access to purchase information, content, music, games and/or eBooks), possibly free news or weather or other modest bandwidth Internet services that are provided free of charge to

entice the user into using/upgrading the service or using the transactions or viewing advertisements, what advertisements are displayed to the user or what advertisement based websites the user is exposed to, certain applications may have access while others are blocked (e.g., Internet based text services have access but email downloads do not), or other example service capabilities. It will be apparent to one of ordinary skill in the art that allowing all of these services, and blocking other ambient user service attempts (e.g., unpaid large file size Internet downloads or uploads or movie viewing or other access that would consume bandwidth and cause the ambient service to be a potential source of losses for the service provider) is made possible by the service profile control capabilities of the service processor and/or the service controller. The bill by account embodiments, as discussed herein, in which each service activity can, for example, be separately tracked with the service monitor and other agents and server functions to produce a billing offset that allows categorization and mediation of different billing entities (accounts) provides the capability for the service provider to individually account for the costs of each ambient service element. This allows business models wherein the free access to the end user is paid for or partially paid for by one or more service provider partners who are billed for service access using the bill by account capabilities (e.g., the transaction partners pay for user access to their transaction experience and perhaps pay a revenue share for transaction billing, the advertising sponsored website partners pay for their access service share).

[0415] While the service control capabilities of the service processor and the bill by account service cost sharing and transaction revenue sharing in some cases can create a profitable ambient business model, in other cases, the ambient services can be a potential source of losses for the service provider. Accordingly, in some embodiments, the ambient service capabilities can be modified over time to reduce service cost to the service provider or VSP based on a variety of decision factors. For example, the user can have one level of traffic control for a period of time, and if the user has not signed up for service by the end of the period, the ambient service access is reduced by changing the service control policy settings in the service processor, and the service level can be further reduced over time if the user continues to not sign up for service or the user does not create much transaction revenue. As another example, the recursive throttling algorithms discussed herein can be utilized to one or more of the service activities offered in ambient service mode so that the user experiences what full speed service is like, and if the user continues consuming appreciable bandwidth with the service activity, then

the activity is throttled back to reduce costs. In these examples, the service processor or service controller can issue the user a notification explaining that their service is currently free so their usage is being throttled, and if they desire to receive better service, service plan upgrade offers can be delivered to the UI. It will now be apparent to one of ordinary skill in the art that the various ambient service parameters, including the provisioning and activation processes used to create the ambient service activation, can also be managed by the VSP apparatus and processes described herein. For example, this allows the same service controllers and service processor solutions to be used to define a wide range of ambient experiences for various device groups or user groups that are controlled by different VSPs.

[0416] Similarly, rather than controlling the ambient service profile settings using the VSP functions to control the service controller, service processor, provisioning and activation settings, other embodiments call for the ambient service profile settings to be controlled by the network based service activity control equipment as similarly discussed herein. Depending on the level of service control and service monitoring sophistication (e.g., highly advanced DPI or service aware techniques), some, much, most or all of the above described ambient services functionality can be implemented using network based service controls and the VSP management and control embodiments described herein.

[0417] In some embodiments, a device is suspended based on inactivity, or the device is placed in a suspended service state or suspended account state, so that the network does not get bogged down with a significant number of devices and credentials that are inactive. For example, this can also result in a portion of the device credentials being assigned back to an available pool rather than reserved for that particular device (e.g., phone numbers if phone numbers are scarce). The device account and/or activation state can be re-activated when the device comes back online. For example, the suspend state can be a simple suspension of services without changing the account status, in which case the re-activation process can be automatically completed as a subset or entire set of the activation sequence that occurs when the device is initially used as described herein. The suspend state can also involve changing the account status to inactive, in which case the re-activation process can automatically reconfigure the account status back to an active state when the device re-accesses the network. For example, the suspend state can involve de-assigning or possibly re-claiming a portion of the device credentials. If a

portion of the credentials are de-assigned, then when the device re-accesses the network credentials can be automatically re-assigned as described in various embodiments described herein.

Network Based Service Monitoring, Notification and Control

[0418] In some embodiments, as described herein, it is desirable to implement some or all of the deep service usage monitoring, service control or control assistance, or service notification or notification assistance associated with a service profile in network apparatus rather than in the device, or to implement some of the deep service monitoring, control, control assistance, notification or notification assistance in the device and others in the network. This is the case, for example, in a mixed network in which some devices have some, or at least one, or all of the service processor capabilities discussed herein, but other devices do not have as much or any of the service processor capabilities. Another example is for networks or devices that do not have any service processor capabilities or where it is desirable to do all of the service monitoring, control and notification in the network rather than the device. As described below, FIGS. 54 through 63 depict various embodiments for combinations of device based service monitoring, control or control assistance, usage notification or usage notification assistance and/or network based service monitoring, control or control assistance, usage notification or usage notification assistance.

[0419] FIG. 54 illustrates a network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments. As shown, an integrated device service control, device usage monitoring system 5410 is provided that integrates service controller functions including a deep packet control (DPC) policy implementation function 5402 with access network AAA server 121 functions and network real-time service usage 118 functions. In the following discussion, it is understood that the AAA server 121 function can be re-located to another point in the network or network equipment partitioning with no loss in generality. It is also understood that many of the functional partitions described for the various embodiments within integrated device service control, device usage monitoring system 5410 can be re-drawn with no loss in applicability, function or generality. Finally, it is understood that one or more of

the functional elements described within the integrated device service control, device usage monitoring system 5410 can be removed for simplified embodiments and that not all the functionality described herein is necessary in some embodiments.

[0420] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service monitoring or control that satisfies various network neutrality and/or privacy requirements based on indication(s) received from the device or user (e.g., user input provided using the device UI using the service processor 115; user input provided through another website, WAP site or portal; or user input provided through the service contract where the user agrees to the monitoring and/or service control levels) and network based service control using a DPI service monitor 5412 and/or the DPC policy implementation 5402.

[0421] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service monitoring or service control that satisfies various privacy requirements using indication(s) received from the device or user (e.g., user input provided using the device UI using the service processor 115; user input provided through another website, WAP site or portal; or user input provided through the service contract where the user agrees to the monitoring and/or service control levels) and network based DPI service usage monitoring or DPC policy implementation using the DPI service monitor 5412 or DPC policy implementation 5402 as described below. In some embodiments, the DPI service monitor 5412 and/or DPC policy implementation 5402 include a secure database for storing service monitoring and CRM information for each device/device user. In some embodiments, the DPI service monitor 5412 and/or DPC policy implementation 5402 can be integrated with the integrated device service control, device usage monitoring system 5410 (as shown) or provided within a separate router, server, and/or software/hardware implemented function that is in secure communication with the integrated device service control, device usage monitoring system 5410 and/or other network elements based on the network architecture. In some embodiments, a secure data store, such as a secure database, is not integrated with the DPI service monitor 5412 or DPC policy implementation 5402 but is in secure communication with the DPI service monitor 5412 or DPC policy implementation 5402, the integrated device service control, device usage monitoring system 5410 and/or other network elements depending on the architecture

(e.g., a billing server or any other network element). In some embodiments, the user selects limits and/or restrictions on who can access remotely stored service usage history and/or other CRM/privacy related data (e.g., CRM/privacy gatekeeper settings), and, for example, other network elements and/or network administrators access to such data can be limited and/or restricted accordingly. For example, access to such stored service monitoring and CRM information can require certain security credentials and/or using various other well known secure data storage techniques, such as the various secure storage techniques described herein.

[0422] In some embodiments, the secure database possessing user service usage information that is considered sensitive and has not been approved for distribution by the user can be made unavailable to the credentials possessed by network managers or network functions except, for example, for emergency service situations of government mandated monitoring needs where special credentials are brought out of secure storage that are not normally available. In some embodiments, rather than the user selecting limits, a certain set of restrictions are assumed unless the user selects information filtering settings that allow more information to be shared with the network functions, network administrators or service provider partners. In some embodiments, the information is filtered to remove information thought to be sensitive but still transmits service usage information needed for monitoring network services or other important parameters. For example, the website destinations a user is visiting can be classified with generic identifiers that are not decodable or the individual website information can be completely removed. Many other examples will be apparent to one of ordinary skill in the art.

[0423] For example, the stored service monitoring and CRM information can also be organized into groups to define group CRM profiles to store service monitoring information for every user indexed by the user credentials (e.g., such groups can also be used for various VSP related functions, as described herein). The DPI service monitor 5412 or DPC policy implementation 5402 also uses the secure storage to store service monitoring information for each user indexed by the user credentials or another aspect of the device identifier or address assignment (e.g., IP address or MAC address). In some embodiments, a CRM information manager (e.g., a supervisor program executing on the integrated device service control, device usage monitoring system 5410) communicates with the other network functions and provides filtered service usage and CRM information according to CRM filtering rules for each user or for

groups of users. In some embodiments, the filtered CRM data can be made available using secure communications with other networking equipment by the integrated device service control, usage monitoring system 5410. In some embodiments, the filter settings for some users allow more information to be shared from the secure service usage information than others due to the differences in user preference settings and/or service plan agreements.

[0424] In some embodiments, user privacy preference information is used to determine the privacy filter settings, which are securely implemented by the integrated device service control, device usage monitoring system 5410. For example, service CRM filter settings can be received at the time of service contract sign up (e.g., service plan selection) and/or allow the user to log into service preferences web page to change settings (e.g., without involving any interaction with local software on the device). As another example, software on the device (e.g., including the service processor 115) can be used for selecting user CRM/privacy preferences, which are securely communicated to the integrated device service control, device usage monitoring system 5410 (e.g., the device can include credentials that can be verified to allow for selection/modification of CRM/privacy preferences or other user based preferences securely maintained in a network server, such as the integrated device service control, device usage monitoring system 5410 or another network element, such as shown in various other embodiments described herein). In these examples, the filtered CRM data is available from the integrated device service control, device usage monitoring system 5410 for other network components over a secure or open communication link. In another example, user CRM/privacy preferences are input using a web server hosted by the integrated device service control, device usage monitoring system 5410 or the central billing system 123. In another example, software on the device (e.g., including the service processor 115) can be used for securely communicating user preference decisions to an intermediate server that acts as a device manager and intermediate server for devices or device groups and the integrated device service control, device usage monitoring system 5410.

[0425] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service control as described below. In some embodiments and similar to the above described network based CRM filtering embodiments, the DPI service monitor 5412 or DPC policy implementation 5402 includes secure storage (e.g., a

secure database) for storing service monitoring information (e.g., based on user selections/preferences), and the DPC policy implementation 5402 performs traffic shaping/throttling algorithms for each user based on the stored service monitoring information from DPI service monitor 5412. For example, network based DPI traffic inspection by the DPI service monitor 5412 can use the secure storage to save service monitoring information for each user indexed by the user credentials or other parameters, such as IP address or other network tag. As another example, the DPC policy implementation 5402, for example, which can be supervised by policy management server 1652 as described herein with respect to various other embodiments, can implement service usage history statistical analysis inside the secure storage and maintain a service usage history analysis for each device/user and/or perform various traffic shaping and/or throttling algorithms based on various device, user selected and/or service plan related settings (e.g., for network neutrality purposes) allowing for various higher level service usage goals for one or more users, as similarly described herein with respect to various device based service usage monitoring embodiments (e.g., except for certain encrypted network traffic flows or application related flows for which traffic control generally needs information from the application level and/or content specific traffic control).

[0426] In some embodiments, input is collected on how to implement service control (e.g., from the user of the device). For example, such input can be determined based on one or more of the following: a service plan choice for the device; input provided by a user via a website (e.g., web based portal) for indicating changes to service control policies, as similarly described above; input provided by a user via the device (e.g., including the service processor 115), which securely communicates the input to the DPC policy implementation 5402, for example, which can be supervised by the policy management server 1652; and input provided by a user via the device (e.g., including the service processor 115), which securely communicates the input to an intermediate server for the DPC policy implementation 5402, as similarly described above. In some embodiments, such service control is based on various algorithms as described herein that identify the heaviest usage service activities and recursively control the speed for those activities while leaving certain others unaffected, and in a manner that is specified or selected by the user to ensure network neutrality. In some embodiments, the user is offered a choice for controlling service usage and/or selects an algorithm that controls all activities equally/neutrally (e.g., based on selected user preferences). For example, by

implementing service control algorithms that are network neutral (e.g., throttling all activities equally or throttling the highest usage algorithms without singling out certain activities for throttling unless they satisfy certain network neutral usage history or usage statistics criteria), or that are approved, selected or otherwise specified by the user, network neutral traffic control or service usage control can be maintained.

[0427] In some embodiments, the DPI service monitor 5412, possibly in conjunction with the service usage notification 5420 and/or service history server 1650, provides service usage/service cost (e.g., a real-time service usage counter) related notifications to the device based on user preferences, as similarly described above with respect to various device based service usage/service related notification embodiments. For example, the DPI service monitor 5412, for example, in conjunction with the service usage notification 5420 and/or service history server 1650, can perform service usage/service related notification algorithms based on one or more of the following: service plans, device settings, and/or user selected preferences (e.g., such notification messages can be securely communicated to the device and/or to the device via an intermediate server). For example, the policies that govern how the user is notified of service usage or service cost can be determined by the policy management server 1652 and/or the service usage notification 5420. As another example, user acknowledgements of important notification messages and/or user choices related to important service usage decisions can be requested, as similarly discussed above with respect to device based service usage/control embodiments, which can then be communicated to the central billing system 123 as confirmation for any such important notification messages (e.g., related to service usage overage charges and/or confirmation of service upgrades). In some embodiments, various other service usage algorithms related to service usage and/or service cost forward projections described herein with respect device based service usage forward projection embodiments are performed in the network, such as by the integrated device service control, device usage monitoring system 5410, and such forward projections can then be communicated to each respective device as service usage notification messages (e.g., using a push based approach (initiated in the network) and/or pull based approach (initiated by a request from the device)). For example, these embodiments for projected service usage methods, as described herein, can be helpful for determining when the user is using services in a manner that will cause the user to run over a service limit so that

the user can be notified, or the service can be controlled or throttled if the user has selected a control or throttling option.

[0428] In some embodiments, one or more intermediate servers are provided for workload balancing and/or off-loading the integrated device service control, device usage monitoring system 5410 and perform one or more of the functions described above with respect to various embodiments of the integrated device service control, device usage monitoring system 5410. In some embodiments, service plans, device settings, and/or user selected preferences are used to associate each device/user with a preprogrammed profile to more efficiently associate such devices/users with their selected service plans, device settings, and/or user preferences. For example, the process of setting a service profile for a given device can be determined by assigning the device to a service flow that has the pre-defined service profile and is shared with other devices within the integrated device service control, device usage monitoring system 5410 rather than individually processing the service flow manipulations for each device. In some embodiments, the act of provisioning and activating a service profile for a given devices involves setting up the service flow definition and identifier within the integrated device service control, device usage monitoring system 5410 (if it is not already set up) and then assigning the routing of the device credentials to that service flow identifier. User preferences can, for example, be accounted for by assigning the device service flow to one of several pre-defined profiles based on user preferences that are all supported under the same service plan. For example, one service flow profile can call for service usage notification but no control under the same service plan as another service flow profile that calls for less notification but active service usage control to maintain user costs to a monthly post-pay limit.

[0429] In some embodiments, the bill by account function is implemented in the context of the integrated device service control, device usage monitoring system 5410 or other network based system embodiments described herein. For example, the DPI service monitor 5412, in some cases in conjunction with service history server 1650, can operate in conjunction with bill by account policy settings stored in the billing event server 1662 so that service activities are divided into the account classifications defined by the service profile settings. The bill by account feeds can then be sent to the billing system or to an intermediate billing event aggregation server that collects this type of deep packet inspection generated information from

one or more integrated device service control, device usage monitoring system 5410 units to aggregate and format the information in a manner that may be used by the central billing system 123. In some embodiments, the bill by account information collected in a network box like the integrated device service control, device usage monitoring system 5410 is augmented by bill by account information collected on the device as described herein, and any intermediate server that can be used to aggregate and format these bill by account feeds for the central billing system deals with both types of data, from the network and from the devices.

[0430] As shown in FIG. 54, in some embodiments, integrated device service control, device usage monitoring system 5410 includes the service control server link 1638, which, for example, can be used as described above (e.g., with respect to FIG. 16 and other embodiments described herein) to communicate with device service processors 115. In some embodiments, billing server 1662 within integrated device service control, device usage monitoring system 5410 detects service usage events reported by DPI service monitor 5412, in some cases in conjunction with service history server 1650, generates a billing event that can be recorded or transmitted to the central billing system 123. In some embodiments, billing server 1662 receives information from device billing agent 1695 and/or device service monitor agent 1696 and transmits the device service usage billing events to the central billing system 123. In some embodiments, certain billing events that are advantageously collected in the network (e.g., DPI service monitor 5412 and/or billing event server 1662) are combined with certain billing events that are advantageously collected on the device (e.g., service monitor agent 1696 and/or billing agent 1695), and both sources of billing information are transmitted to the billing system 123. Similarly, in some embodiments, certain service usage information is collected with service usage monitor agent 1696, and that information is combined with service usage information collected from DPI service monitor 5412 and/or service history server 1650 and/or service usage 118. In some embodiments, certain service aspects are controlled using network based DPC policy implementation 5402, in some cases in conjunction with or supervised by network based policy management server 1652, and other service aspects are controlled using device based policy implementation agent 1690, in some cases in conjunction with or supervised by policy control agent 1692. As will now be apparent to one of ordinary skill in the art in view of the numerous embodiments described herein, many hybrid approaches to service usage monitoring, service control, service notification or service billing can be accomplished with some aspects of

the policy, notification, control, monitoring or billing being implemented/performed on the device apparatus described herein and others implemented/performed on the network apparatus described herein. The presence of access control integrity server 1662 and many other service control verification embodiments described herein make it apparent that the integrated device service control, device usage monitoring system 5410 embodiments also provide for affirmative verification of whatever functions are implemented on the device. It will also be apparent that all of the above combinations of device and network functions, and many others, can be accomplished in ways that are network neutral and/or protect user privacy preferences by implementing the service control algorithms in a network neutral manner and/or receiving user preference input on how to implement service control, and by maintaining service usage and CRM information security and filtering on both the device 100 and the network based integrated device service control, device usage monitoring system 5410.

[0431] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates or plays a part in automated provisioning and activation of the devices as similarly described above with respect to various device based automated provisioning and activation embodiments. In some embodiments, the activation server 160 is integrated into or partially integrated into device service control, device usage monitoring system 5410.

[0432] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates ambient services as similarly described above with respect to various device based ambient services embodiments.

[0433] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates VSP and ODI solutions as similarly described above with respect to various device based VSP and ODI embodiments.

[0434] Various other network architectures for network based service control including deep packet inspection functions can similarly be used as will be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[0435] FIG. 55 illustrates another network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments. As shown, the service processor 115 is not present on the devices 100, and the integrated device service control, device usage monitoring system 5510 performs all service monitoring, service control, billing, and notification functions.

[0436] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments. As shown, a 4G/3G/2G DPI/DPC enabled gateway 5610 (e.g., implemented in either gateway 420 or gateway 410 or a combination of both) where the conventional service gateway functions 5616 (e.g., routing, switching, protocol translation/tunneling, charging data function (CDF), charging gateway function (GCF), mobility management, and/or suspend/resume) are combined with one or more of the following embodiments and integrated into one or a combination of the service gateways (e.g., RAN and/or transport gateways): DPI service monitor 5412, service history server 1650, device usage 118, DPC policy implementation 5402, policy management server 1652, user notification 5618, billing event server 1662, access control integrity server 1654, service control service link 1638, data plane I/O 5612 (e.g., used to represent the I/O port(s) for the gateway), and/or DPI/DPC gateway control plane link 5622 (e.g., used to represent the control plane network channel connecting the above elements to other network equipment and in communication with gateway control communication 5620). The packet processing architecture shown in this figure calls for a multi-point to multi-point backplane bus scheme, but it will be apparent that other data path configurations are possible including serial. As will also be apparent, the above described configuration can also be applied to either the transport gateway 420 and/or the RAN gateway 410. As mentioned above, it is possible to maintain a secure storage on the 4G/3G/2G DPI/DPC gateway 420 or 410 that requires secure credentials to get into so that user privacy is protected and service usage information or CRM information is filtered according to user preferences prior to sending to another network function or network manager, and the same allowances can also be applied for emergency or government monitoring purposes. Network neutrality can also be maintained in this configuration by maintaining network neutrality in the service control algorithm and/or soliciting user input on how to control service usage just as discussed above for other network service control implementations or as discussed in the device based service control descriptions.

[0437] In some embodiments, the bill by account function is implemented in the context of the 4G/3G/2G DPI/DPC gateway 5610 embodiment or other network based system embodiments described herein. For example, the bill by account information can be completely derived from the network box (e.g., 4G/3G/2G DPI/DPC gateway 5610) without assistance from device based service monitoring or billing capabilities, or none may exist on the device. In this example, the DPI service monitor 5412, in some cases in conjunction with service history server 1650, can operate in conjunction with bill by account policy settings stored in the billing event server 1662 so that service activities are divided into the account classifications defined by the service profile settings. The bill by account feeds can then be sent to the billing system or to an intermediate billing event aggregation server that collects this type of deep packet inspection generated information from one or 4G/3G/2G DPI/DPC gateway 5610 units to aggregate and format the information in a manner that can be used by the central billing system 123. In some embodiments, the bill by account information collected in a network box, such as the 4G/3G/2G DPI/DPC gateway 5610, is augmented, refined or otherwise added to by bill by account information collected on the device as described herein and any intermediate server that can be used to aggregate and format these bill by account feeds for the central billing system deals with both types of data, from the network and from the devices.

[0438] FIG. 57 illustrates a network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420 in accordance with some embodiments. As shown, the VSP workstation server 4910 is in communication with the 4G/3G/2G DPI/DPC gateways 410 and/or 420, the Service Controller Design, Policy Analysis, Test, Publishing System 4835, and/or other networking elements including possibly the central billing system 123, the mobile wireless center 132 (HLR) and/or the AAA server 121 for the purpose of provisioning and/or controlling settings in the 4G/3G/2G DPI/DPC gateways 410 and/or 420, the mobile wireless center 132 and possibly other equipment for the purpose of implementing a portion of the VSP open partner functionality discussed herein. In FIG. 57, the 4G/3G/2G DPI/DPC gateway 5610 functionality as shown in FIG. 56 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420 as similarly described above. For example, the VSP functionality can also be used to set higher level policies associated with the 4G/3G/2G DPI/DPC gateway 420 or 410, such as provisioning or activation profiles or policies, ambient service profiles or policies, and/or bill by account

service profiles or the other higher level service profile or service plan embodiments discussed herein. In some embodiments, the provisioning and/or activation steps described herein involve setting service policies in the 4G/3G/2G DPI/DPC gateway 420 or 410. In some embodiments, ambient services or ambient activation involve setting up service profiles within the 4G/3G/2G DPI/DPC gateway 420 or 410 that allow the desired activities and block the undesired activities. For example, these settings can be included as part of the open service provider partner programming capabilities of the VSP workstation server 4910 embodiments.

[0439] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments. As shown, a 4G/3G/2G DPI/DPC gateway 5810 (e.g., implemented in either gateway 420 and/or gateway 410) is provided in which the service processor connection (e.g., via service control server link 1638 as shown in FIG. 56) is not present so that all service monitoring, control, billing event collection and transmission, and notification are performed by the 4G/3G/2G DPI/DPC gateway 5610 (e.g., gateways 410 and/or 420).

[0440] FIG. 59 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, the AAA 121 and the mobile wireless center 132 in accordance with some embodiments. As shown, FIG. 59 provides a network diagram corresponding to FIG. 58, with similar functionality to the embodiment shown in FIG. 57, in which the service processors 115 are not present on the devices 100. In FIG. 59, the 4G/3G/2G DPI/DPC gateway 5810 functionality as shown in FIG. 58 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420 as similarly described above.

[0441] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments. In some embodiments, enhanced network based service monitoring, control, billing and notification as discussed above is implemented using a 4G/3G/2G DPI/DPC enabled gateway 6010 and service controller device control system 6025 as shown. In some embodiments, the functions shown in the figure to be inside of the service controller device control system 6025 have been moved from the 4G/3G/2G DPI/DPC gateway 5610 of FIG. 56 (e.g., or from gateways 410 and/or 420) so that they reside in a separate server embodiment or other network equipment function separate from the 4G/3G/2G

DPI/DPC gateway 6010. For example, this architecture can be used when the network equipment manufacturer desires to separate these functions or has an existing product that it is desirable to upgrade by adding a separate box. As another example, this architecture can be used when the 4G/3G/2G DPI/DPC gateway 6010 is not capable of keeping up with large numbers of individual user profiles so it is desirable to go to a scalable server configuration in which load balancing can be applied with a potentially more flexible programming environment for implementing service policy management functions, statistical service history analysis algorithms, service usage projection, and/or service control (or throttling) algorithms. In some embodiments, a secure storage is provided on the 4G/3G/2G DPI/DPC gateway 6010 and/or the service controller device control system 6025 that requires secure credentials to get into so that, for example, user privacy can be protected and service usage information or CRM information can be filtered according to user preferences prior to sending to another network function or network manager, and the same allowances can also be applied, for example, for emergency or government monitoring purposes. For example, network neutrality can also be maintained in this configuration by maintaining network neutrality in the service control algorithm construction and/or soliciting user input on how to control service usage just as discussed above for other network service control implementations or as discussed in the device based service control descriptions.

[0442] FIG. 61 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, AAA 121 and mobile wireless center 132 in accordance with some embodiments. In FIG. 61, the 4G/3G/2G DPI/DPC gateway 6010 functionality as shown in FIG. 60 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420, as similarly described above, and which are in communication with the service controller device control system 6025 as shown.

[0443] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments. As shown, the capability to communicate with the service processor 115 has been removed so that all service monitoring, control, billing event collection and transmission, and notification are performed by the 4G/3G/2G DPI/DPC gateways 6210 (e.g., implemented in gateways 410 and/or 420) in

conjunction with the service controller device control system 6225 without assistance from the service processors 115.

[0444] FIG. 63 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, AAA 121 and mobile wireless center 132 in accordance with some embodiments. In FIG. 61, the 4G/3G/2G DPI/DPC gateway 6210 functionality as shown in FIG. 62 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420, as similarly described above, and which are in communication with the service controller device control system 6225 as shown.

[0445] As will be apparent to one of ordinary skill in the art, the above described embodiments can be extended to include some or all of the functions depicted in the 4G/3G/2G DPI/DPC service gateways of FIG. 56 in the base station or base station controller 125.

Provisioning and Activation

[0446] In some embodiments, automated provisioning and activation includes automation of one or more of the following functions: (1) programming device credentials or partial credentials and recording them in a database (or providing same when they are programmed into the device), (2) associating these credentials with the proper provisioning and/or activation actions to be taken on the device and in the network, (3) directing the device to the proper activation function (e.g., activation server) sequence when it attempts to connect to the network, (4) completing provisioning of the device, (5) programming the AAA, billing system, gateways, mobile wireless center and other network equipment to the proper initial device service control settings, and (6) establishing a service account for the device.

[0447] In some embodiments, improved processes for activating service for a device or user with a network service provided by a central provider network, an MVNO network or a VSP on the central provider network are provided. In some embodiments, activation includes one or more of the following: a process or result of associating a service account with device or user credentials; with the service account potentially further being associated with a service profile defining the service activities that the device is authorized to access; creating or updating

a service usage or billing record and associating it with the service account to create a service plan; and/or initiating service to the device or user in which the network equipment allows access to the appropriate level of service activities. In some embodiments, VSP embodiments include the provisioning and activation apparatus embodiments of any or all forms.

[0448] In conventional mobile device provisioning systems, the provisioning and activation process required to create a user service account and enable the device to access the desired level of service activities can limit mass market, low cost or user friendly applications of the device or service, because the process can often be cumbersome, time consuming and/or expensive for the service provider, service owner, master agent (service distributor), MVNO, VSP and/or user. Accordingly, the various embodiments for provisioning and activation described herein simplify the provisioning and activation process for mobile devices. In some embodiments, provisioning and activation for the device and/or the network accommodates a wide variety of device types and service profile types, with the capability to perform the provisioning and activation at a number of points in the manufacturing, distribution, sales and usage progression for the device, and the ability to either pre-activate before first device use or very quickly activate during first device use (or during some later use of the device).

[0449] In some embodiments, as described herein, the term provisioning generally refers to those actions/processes associated with programming the device with credentials or other device settings or software installations used to later activate the device, as well as, in some embodiments, creating database entries and other credential associations in the network so that the network and/or device have the information used to recognize the device or credentials and implement the service policies in the service profile and/or service plan once the service profile and/or service plan are activated. In some embodiments, as described herein, the term activation generally refers to the process of creating or selecting the service plan and/or service profile, programming the settings that are used in each (e.g., required) network function and/or each (e.g., required) device function so that the system can properly associate the device credentials with the appropriate service activity policies, and then admitting the device onto the network. The term activation can also refer in some embodiments to the creation of a user or device service account, in some cases, with user or device owner information or billing information. In some embodiments, the process of provisioning amounts to assigning credentials to the device

and programming a portion or all of the credentials on the device, entering a portion or all of the credentials in the various necessary network equipment databases so that the network components are capable of identifying the device and associating it with the network based portion of the admission, traffic processing, service monitoring, billing, service limits and other policies that are eventually defined by the service profile and service plan.

[0450] Further examples of the network based service profile policies include network access level, traffic routing, service monitoring, service limits and actions taken upon reaching service limits. Once the service profile is created and activated during the activation process, the device credentials and the associated service profile are communicated throughout the necessary network elements so that each element can implement its part of the network portion of the service profile policies. This process of propagating the service profile settings to all the required network equipment components is a portion of what is referred to herein as activation in accordance with some embodiments. In some embodiments, the activation process includes associating the credentials with the proper service plan and/or service profile, and possibly completing the process of programming the device functions and/or network functions so that the device can be admitted to the appropriate level of network services. In some embodiments, activation also includes the service processor software settings, configurations or installs for each function or agent in the service processor to implement its part of the service profile, service plan, service billing or transaction billing policies. In some embodiments, activation also includes the creation of entries in the various service account databases and/or billing databases to create a user account or device owner account for the purpose of managing the user choices for service plan and other account information storage and management aspects, such as maintaining status information, maintaining the central service profile configuration, conducting reconciliation and billing exchanges, service usage history, and/or account history.

[0451] In some embodiments, the term credentials generally refers to the set of information parameters that the network and/or device uses (e.g., requires) to admit the device onto the network and associate it with the appropriate service profile and/or service plan. For example, the credentials can include one or more of the following: phone number, device identification number, MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or

credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version, device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider, OEM, master agent (service distributor), VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user. In some embodiments, at least some of the credentials are unique to the device, and, in some embodiments, groups of devices share one or more aspects of the credentials. In some embodiments, the term permanent credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a permanent basis. In some embodiments, the term temporary credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a temporary basis. In some embodiments, temporary credentials are eventually replaced by permanent credentials. In some embodiments, at least some elements in the temporary credentials (e.g., phone number and/or access or authorization security credential) are used for more than one device. In some embodiments, the temporary credentials are recycled from one or more devices and used for one or more other devices, for example, when they remain unused for a period of

time or when they are replaced with permanent credentials on one or more devices. It should not be inferred from the term permanent credentials that permanent credentials are never recycled, for example, when the user discontinues service or use of the credentials. Also, the term temporary credentials does not imply that temporary credentials are always temporary. In some embodiments, partial credentials or pre-activation credentials generally refer to a subset of credentials that are to gain access to limited network services for the purpose of provisioning of credentials and/or activation of a service plan or service profile. For example, prior to a phone number being assigned, a device can gain access to a limited set of network server destinations in which embedded information contained in the device (e.g., the partial credentials) is provided to the server, the server associates that information with the proper additional credentials (including the phone number) to assign to the device and/or associates the information with the proper service profile to activate service. In this example, partial credentials can include device type, OEM, service provider, VSP, device identification number, SIM, service processor configuration or some other information used by the server to determine what the credentials should be and the proper service profile.

[0452] In some embodiments, a permanent service account generally refers to the service account that is permanently associated with the user and/or device. For example, this account includes an association with the device or user credentials, user information or billing information, service profile, billing profile, network authorization status and other aspects that define the device or user service policies and billing policies. In some embodiments, the term temporary service account generally refers to a service account that is temporarily set up and associated with the device before some or all of the required permanent account information is available or entered for a device or user. For example, this account can be set up with an association with an actual user, or can be set up with a mock user or unassigned user association so that the network and billing system can recognize the credentials, authenticate the device, admit the device, provide the proper level of service activity control according to the service profile associated with the temporary service account, or collect the service activity usage information for various network and billing system accounting needs before actual user information or billing information has been entered into the network systems. For example, a temporary service account can make it possible or easier to use existing billing systems or other network systems to provide simplified provisioning, simplified activation or ambient services. A

temporary service account can also become a permanent service account by replacing mock user or unassigned user information with actual user information, or a temporary service account may need to be replaced by a permanent service account when actual user information needs to be entered into the network systems, possibly including the billing or service profile databases.

[0453] In some embodiments, temporary or permanent device credentials and other information used/required for provisioning the device are generated with apparatus located at the manufacturer or in the distribution channel as discussed below. In some embodiments, the apparatus includes a local onsite server that typically shares some aspects of the provisioning information (e.g., phone number, phone number range, MEID or MEID range, SIM number or SIM number range, IP address or IP address range, MAC address or MAC address range, other secure device credential elements) with a network provisioning database. In some embodiments, the apparatus includes a server terminal, and the aforementioned portion of the credentials is generated by the network and shared with the local provisioning apparatus. In some embodiments, as will be discussed below, the provisioning credentials are in part generated in the network and shared with the device while it is connected online to an activation server (e.g., activation server 160) that is connected to the access network. Similarly, there can be activation servers connected to apparatus in the manufacturing or distribution channel that service device activation, or over the air or over the network apparatus connected to an activation server, which in turn connects to the device, can be used to accomplish activation programming of the network and device as further discussed below.

[0454] In some embodiments, when a device is provisioned and entered into the network provisioning database, it is associated with the automatic provisioning and/or activation sequence the device is intended to go through once it connects to the network or to the apparatus that will complete the process. In some embodiments, one or more device parameters (e.g., service owner, device type, OEM, plan type, IP address, security credential and/or software version) are used to determine what the appropriate network provisioning steps and/or settings are for completing the provisioning and/or activation process, and this association information is stored in the network provisioning database for propagation of the provisioning profiles or activation profiles to the various network equipment elements. In some embodiments, the network provisioning database is provided (e.g., in the network) that associates the pre-activation

provisioning information (e.g., generated, as described herein, at time of manufacture, sometime during distribution, by the user on a website by a sales associate or other activation assistant, or by the network when a new device enters the automatic activation process). For example, the pre-activation provisioning information informs the network whether or not to let the device onto an activation sequence when the device attempts access, and in some cases, also instructs the network to direct the device to a specific activation sequence including, for example, an activation server (or other activation sequencing apparatus) sequence as described herein. In some embodiments, a central database is queried by other network equipment or the central database is included in one or more of the network elements (e.g., the AAA server and/or billing system, mobile wireless center 132), or the database is copied in part or in whole in various network elements (e.g., the central database, AAA server, mobile wireless center, billing system and/or gateways).

[0455] In some embodiments, propagating the network equipment provisioning information for a given device or group of devices is accomplished with a network provisioning system that has access to the network provisioning database and is capable of programming the appropriate network equipment. In some embodiments, this network equipment is referred to as “network management” equipment or “network provisioning” equipment. In some embodiments, there are several functions that take part individually or in concert, including, for example, the AAA server 121, service controller 122 (either with device based/assisted services through the service processor related embodiments or with network only embodiments as described herein), the mobile wireless center 132 (e.g., including the home location register (HLR) or other similar function referred to by other industry terms), the activation server(s) 160, other network provisioning or management equipment attached to or associated with the billing database system, and/or some other equipment apparatus. In some embodiments, the local database on the device, database in the AAA server and/or database elsewhere in network is provisioned to inform the gateway of the process for handling the pre-provisioned device according to, for example, the credentials. For example, if the device is not recognized or not authenticated onto the access network as an activated device with associated active service profile and/or service plan, the device connection or communication can be directed (or routed) to a generic activation server that provides an activation sequence that is not necessarily determined by one or more of the specific device credential elements, partial credential elements,

device profile or partial device profile that define something specific about the activation sequence for the device. In another example, in which the device is not recognized or authenticated as an activated device with associated service profile and/or service plan, the device can be directed (or routed) to an activation service (or other activation sequencing apparatus) that uses some part of the credentials or range of partial credentials or a portion of a partial or complete device profile to determine a desired pre-determined device specific or device group specific activation sequence that is implemented by a specific activation service sequence or other activation sequence apparatus. In another example, in which the device is not recognized or authenticated as an activated device with associated active service profile and/or service plan, a portion of the device credentials or partial credentials can be used as a look-up index into a database that determines what the specific device activation sequence should be, and the device can be directed (or routed) to a specific activation server sequence or other activation sequencing apparatus.

[0456] In some embodiments, a database in the AAA server or database elsewhere in network is provisioned to inform the gateway what to do with a pre-provisioned device according to the credentials. For example, devices can be authenticated (for activated devices), routed to activation servers (or other activation sequencing apparatus) or denied access. In some embodiments, the AAA server (and/or other network elements) provide the above discussed look-up function for the above gateway description in which a lookup database, locally stored or stored in a central database, is queried to provide secondary routing information to the specific or generic activation servers.

[0457] In some embodiments, the pre-provisioned database is located in the billing system. In some embodiments, the billing system accesses the pre-provisioned database (e.g., stored on the billing system or another network element) for the purpose of setting up temporary accounts or permanent accounts and associating those accounts with pre-activation status, activated free ambient or activated paying customer.

[0458] In some embodiments, for zero activation, all the required pre-provisioning or programming of the above network elements, or others, is coordinated by the network provisioning system at some point after the partial or full device credentials have been associated

with the device or reserved for a particular device type or service type. In some embodiments, the network provisioning system also coordinates the information to or from the device provisioning apparatus that is described elsewhere.

[0459] In view of the various embodiments described herein, it will be appreciated that many of the automated or background provisioning, activation and ambient embodiments described herein can be accomplished with network based approaches, device based approaches, or network/device combination/hybrid based approaches. For example, when the access control for the provisioning process is accomplished in the device (e.g., a device based approach), the activation server can be located anywhere on the Internet, and the device will ensure that the activation process is conducted with the activation server while blocking other traffic from occurring. As another example, some or all of the ambient provisioning programming steps become steps to program the access control, traffic control, application control, bill by account rules, and/or other aspects in the service processor or service controller as described herein.

[0460] In some embodiments, the provisioning apparatus described herein can be a computer located in the user's home or business, and the user or an IT manager has access to a website that provides the provisioning information, in which the computer serves as the provisioning or software programming apparatus. In some embodiments, the network itself, possibly through an activation server 160, website or other interface to the device, becomes the provisioning apparatus, in some cases, with the assistance of software on the device to affect the programming of provisioning information from the network or the communication of device credentials or other information to the network. For example, this software can be a background process that runs without user interaction, a portal/widget program, a web browser based program, a WAP browser based program, and/or any other program that provides a counterpart function to the network functions effecting the provisioning (e.g., activation server). In some embodiments, the activation server either initiates a specific provisioning sequence if device software is present to assist or routes to a website for manual entry if there is no software present.

[0461] FIG. 64 illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial

provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments. Device credential, software and settings server 6420 provides a link to the network functions that generate or provide device credentials, and/or associate device credentials with activation profiles or pre-activation profiles in the network equipment (e.g., the billing system 123, service controller device control system 6225, gateways 410, 420, base station 125, credential generation and association server 6410, activation server 160, service download control server 1660 and/or other network apparatus). For example, the link between the device credential, software and settings server 6420 to the central provider core network equipment can be over the Internet 120 (e.g., a secure link over the Internet) as shown or over another connection such as a leased line. The device credential, software and settings server 6420 obtains credentials or partial credentials from the network apparatus that generates them, illustrated by the credential generation & association server 6410. Credential generation & association server 6410 need not be directly connected to the central provider core network 110 as shown, but can be located elsewhere (e.g., in another location connected by a secure Internet link). Credential generation & association server 6410 assigns credentials, or partial credentials, for use by device credential, software and settings server 6420. When these credentials are assigned to a device, they are programmed, loaded or otherwise associated with the device by device credential provisioning apparatus 6430, which is connected to the device wirelessly or via a wire line connection.

[0462] In some embodiments, a device software loading and programming apparatus 6440 provides software loading or device settings functions that form a portion or all of the provisioning or pre-provisioning device configuration, or form a portion or all of the device activation profile configuration, or form the device service owner, master agent or VSP device assignment or signature, and in some embodiments, using an activation tracking service (ATS) system. As discussed herein, the ATS monitors network connections and aspects of traffic that provide insight into which networks the device 100 is gaining access to, in some embodiments, for the purpose of ensuring that an OEM, master agent, device service owner or VSP is being compensated for devices that activate on a service provider network. In some embodiments, the ATS agent connects to a server counterpart that records and, in some embodiments, also analyzes the service or network connection information to make a determination of the type of access service the device is receiving and, in some cases, determine which networks the device is

activated on. In some embodiments, the ATS is installed on the device in a manner that makes it difficult to tamper with or remove so that the entity that is intended to get credit for device service activation does get credit (e.g., the ATS agent can be loaded into secure memory, it can be installed with software that makes it difficult to de-install, it can be installed on the modem possibly in secure memory, it can be installed in the BIOS, it can be installed deep in the OS kernel, it can be installed with one or more additional device agents that monitor the ATS agent and alert a network function or re-install it if tampered with). The SIM inventory 6450 is provided to illustrate that, in some embodiments, hardware elements (e.g., a SIM security module as shown) or hardware configurations are also installed or manipulated in device 100 and these operations and the recording of the resulting associations form a portion of the provisioning or pre-provisioning process.

[0463] In some embodiments, at the time the credentials or partial credentials are loaded, programmed, set, installed, read from the device or otherwise recorded, they are, in some cases, all associated together in a database that allows for later identification of the device and its appropriate provisioning and/or activation process through such associations. For example, this can involve reading device parameters such as MEID, MAC address, device type, or other information that is associated with the information being loaded or configured on the device. As discussed herein, this credential configuration and association information is stored in the network equipment responsible using it to configure the network to activate the device in one of the various embodiments disclosed herein.

[0464] Some embodiments include tying some or all of the activation provisioning steps and information settings together into a database that defines a higher level activation profile for a group of users(/devices), and a server is used to perform device and equipment programming for the devices in the group, including, for example, associating the following device information into the group definition: credentials, service owner or master agent, provisioning information and/or activation profile. Some embodiments further provide for this device group information being distributed to the various network equipment components required to activate the devices as discussed elsewhere. In some embodiments, this programming and device group association is accomplished using the VSP workstation server 4910. For example, a device can be

manufactured and distributed in a manner that provides flexible assignment of the device to a group that is assigned to an activation profile or a service owner.

[0465] In some embodiments, multiple activation servers 160 are provided (as shown), which illustrates that there can be multiple device activation servers 160 each with a different device activation experience and potentially controlled by a different VSP, service owner, service provider, OEM or master agent. As discussed herein, there are several ways that a device 100 can be routed to the proper activation server 160 so that the device provisioning and activation process can be completed. In some embodiments, all devices that are not activated are re-directed (or routed) to an activation server that reads one or more parameters in the device credentials. The device credential information can be determined either through the device identification information associated with the access network connection itself (e.g., MEID, IP address, phone number, security credentials, or other credentials identified for a device that gains access with the network), or with the aid of the device in a pre-arranged query-response sequence. The device can then be re-directed (or routed) to the appropriate activation server for that device, device group, device service owner or VSP. In some embodiments, the same process described above can be accomplished with a single re-direction from a service gateway 420 or 410, or another router enable network element. In some embodiments, the gateway or network element itself decodes the device credential information as described herein and performs the correct re-direct (or route) to the appropriate activation server 160 for that device. In some embodiments, the activation server 160 can be incorporated directly into the gateway 420 or 410, the base station 125 or other network component. In some embodiments, the activation server 160 can be incorporated into the service controller 122 or the service controller device control system 6225.

[0466] In some embodiments, apparatus other than the activation server are used to facilitate provisioning of credentials or partial credentials, or activation, during manufacturing or device distribution, and, for example, these apparatus can augment, supplement, compliment or replace the activation server function. Such apparatus include, for example, device programming equipment (e.g., device credential provisioning apparatus 6430, device software loading and programming apparatus 6440 or SIM inventory 6450), equipment that is networked into a central provider, MVNO or VSP database (e.g., device credential, software and settings server 6420) to

gain access to provisioning information or activation information that is programmed into a device or group of devices, or to place device credential or partial credential information in a network database for later recognition, or to receive or communicate security information such as certificates for devices or SIM modules that will later be used to complete provisioning or complete activation or gain access to a network. For example, these apparatus, or any other apparatus including the activation server, can be networked into a service provider network or device database, an MVNO network or device database or a VSP network or device database. In some embodiments, programming of the device credentials or other information associated with the service processor or device is provided, so that, for example, the device can be recognized by an activation server or similar network function at a later point in time so that provisioning or activation can be completed in an automated manner, potentially with reduced or no user involvement, that provides a provisioning or activation configuration that is in some way unique for the service provider or service provider partner, device type, user group, VSP, MVNO, master agent or other entity. In some embodiments, this programming is provided in a manner that is difficult to change without the proper authorization so that the device is properly associated with the proper “service owner” or master agent (e.g., for the purpose of activation incentive payments). For example, as discussed herein, various approaches can be applied to the device credential or other settings or software provisioning so that the settings or software are secure or protected, or so that if the software is removed, replaced or modified it is reported or replace or restored. In some embodiments, VSP control of the provisioning, partial provisioning or activation of devices is provided during manufacture or at different points in the distribution channel. As discussed herein, some of these embodiments allow the central provider to offer to service partners (e.g., VSPs, MVNOs, master agents, and/or OEMs) similar types of control for device activation experience design or device service assignment control (e.g., sometimes referred to as service provider device locking so that other service providers cannot provide primary access to the device) during the manufacturing or distribution process that are possible with devices manufactured and distributed for the central service provider.

[0467] In some embodiments, the device is provisioned before the user obtains the device with permanent credentials, temporary credentials or partial credentials. In this case, the necessary credential programming of the device occurs during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of

shipment. In some embodiments, provisioning of network information as discussed above is used, and the network information is provisioned at the same time, before or after the device information is provisioned. In some embodiments, the device provisioning information is programmed with dedicated apparatus that connects to the device either with wires or wirelessly. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or it can be partially or entirely networked into a database or provisioning solution located elsewhere and operated by the central provider, a VSP, OEM or other entity. For example, the apparatus to program the network portions of the provisioning information can also be networked and the operators who set up the required network programming for a device or group of devices may be in the vicinity of the servers that host the provisioning and management tools or they may network into the servers. In some embodiments, provisioning system operators have full or partial control of any device provisioning equipment associated with the entity they work for (e.g., OEM, VSP or master agent) but only have remote access via secure terminal, secure website or other techniques to network into a central provider or VSP server farm in which they control or partially control the network portion of provisioning capabilities for that subset of devices that are assigned to the entity they work for with (e.g. OEM, VSP or master agent).

[0468] In some embodiments, provisioning is accomplished over the air on the mobile access network for mobile devices, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment, such as a computer to perform the programming required to complete provisioning. In the cases in which the device is provisioned at point of sale or after point of sale, the device provisioning can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, in some embodiments, partial credentials that include information such as device type, OEM or service provider are used to assist in determining how to complete the provisioning, and the information can also include secure information, certificate or signature programmed into the partial credentials that is required for the network to perform the provisioning of the remaining credential information in the device and possibly the network. In some embodiments, any network information

used/required to provision the device or service is generated at the time the partial credentials are determined rather than beforehand.

[0469] In some embodiments, the device is activated for service before the user obtains the device with permanent credentials, temporary credentials or partial credentials, or with a permanent service account or a temporary service account. For example, in this case, the necessary steps of provisioning and activating service for the device can occur during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of shipment. In some embodiments, the steps for activating service include one or more of the following: provision the device (e.g., with permanent, temporary or partial credentials), provision the necessary network databases and equipment to prepare them to recognize the device and associate it with the service profile and/or service plan, create or select the service account (e.g., permanent or temporary service account), select or create the service profile and/or service plan, program any elements in the device required to activate service (e.g., account ID, device aspects of the service profile and/or service plan), and program the necessary network databases and equipment with the required associations of device credentials and service profile and/or service plan policy settings. In some embodiments, the device oriented programming portions of the service activation steps occur at the same time, before or after the network oriented programming portions of the service activation steps.

[0470] In some embodiments, the device activation information is programmed with dedicated apparatus that connects to the device via a wireless or wire line connection. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or the dedicated apparatus can be partially or entirely networked into a database or service activation solution located elsewhere and operated by the central provider, a VSP, OEM or other entity. For example, the apparatus to program the network portions of the activation information can also be networked and the operators who set up the required network programming for a device or group of devices can be in the vicinity of the servers that host the service activation and management tools or they can network into the servers. In some embodiments, activation server tools operators have full or partial control of any device activation apparatus associated with the entity they work for (e.g., OEM, VSP or master agent) but only have remote and partial access via secure terminal, secure website or other techniques to

network into the network portion of the activation tools that are controlled by the central provider or VSP. The server tools operators can be restricted in some embodiments to providing network activation information or settings only for those devices or device groups that are assigned to the entity they work for with (e.g., OEM, VSP or master agent). For example, the device control group restriction can be accomplished with a secure database that has secure sub-partitions for one or more entities so that they cannot impact the control of one another's network activation settings but can control their own devices. In this way, a centralized set of activation tools resources controlled by a central provider, VSP or other entity can be partitioned so that different entities can have partial or full control of the activation service definition for devices or groups of devices without impact or risk to others who share the network and activation tools resources.

[0471] In some embodiments, activation is accomplished with an over the air interface to a mobile device, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment such as a computer to perform the programming required to complete activation. In the cases in which the device is activated at point of sale or after point of sale, the final device activation process can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, some embodiments call for a temporary service account that is used to bring the device onto the network before the user has input the information necessary to create a permanent service account. In some embodiments, a temporary or permanent service account can be applied to the device at the time the device reaches the network, and the type of account, service profile and/or service plan can be influenced (e.g., partially determined or informed) or determined by information embedded in the device credentials or partial credentials, such as device type, device ID, SIM, OEM or service provider. For example, the device credentials can also include secure information, certificate or signature that can be required by the network to perform the activation steps for temporary or permanent service account status. In some embodiments, in which the device is activated in this manner before the user information is available, or before the user has selected a pay for service plan, the service profile and service plan are set up for ambient services as described herein.

[0472] In some embodiments, the device is activated during the manufacturing or distribution process, and then the activated device status is suspended. Once the temporary or permanent service account is set up, with appropriate service profile and/or service plan and temporary or permanent credentials, in some networks and billing systems the service can often be more easily resumed once suspended as compared to provisioning and activating the device from scratch. The device is then later resumed (or re-activated) when some event triggers the resume process, such as when it ships to the end user or when the end user attempts to use it. This process prevents the network from needing to manage credentials and accounts for devices that have been activated but are not yet on the network.

[0473] In some embodiments, provisioning is accomplished at least in part with temporary credentials in a manner which is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary credential elements replaced at a later point in time by permanent credential elements in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary credential set is pre-programmed into the device along with a temporary or permanent service account including service profile during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming is performed for the network via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, a subset of the temporary credentials is recycled once it is replaced, if a temporary service account is not activated or used after some period of time, if a permanent account is not activated or used after some period of time, or if the credentials subset is revoked from the device for some other reason.

[0474] In some embodiments, more than one device is assigned one or more elements of the temporary credentials, such as the phone number, which may be limited in supply. In some embodiments, a network will accept more than one set of temporary credentials, one or more redundant elements, for two or more different devices. In some embodiments, a device that has two or more temporary credential sets, in which at least a subset of the credential elements are different for the sets, so that if one set of credentials has elements that are already being used to

access the network, then one or more reserve sets can be drawn upon to gain access to the network.

[0475] In some embodiments, the temporary credentials are used to log onto the network to conduct an over the air or over the network activation process in which an activation server reads at least a portion the device credentials to determine some aspect of how the device service profile. In some embodiments, the aforementioned over the air activation process is accomplished in the background without user intervention. In some embodiments, the over the air activation process is initiated when the user first attempts to use the device or when the user first attempts to access the network or upon user request or approval. In some embodiments, the over the air activation process is initiated using a temporary service account for the device and/or network to gain access to the network. In some embodiments, the over the air activation process is initiated after the user has entered the information required to create a permanent user account into the device or into the network. In some embodiments, the user is required to enter the aforementioned user information before using the device or using some aspect of the device. In some embodiments, the temporary service account is replaced by a permanent service account some time after the user has entered the necessary information to create a permanent account into the device or network. In some embodiments, the over the air activation process is initiated using a permanent service account assignment for the device and/or network to gain access to the network.

[0476] In some embodiments, the service profile is assigned to the device and/or network during the aforementioned over the air activation to be a pay for service profile with a free trial period. In some embodiments, the service profile assigned to the device and/or network during the aforementioned over the air activation includes pre-pay, post-pay, session based pay or pay as you go options for service. As will be apparent to one of ordinary skill in the art, various embodiments disclosed herein are particularly well suited for control or pre-pay services. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned over the air activation is an ambient service profile providing service access before all the user information is available to assign a permanent account. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing a service upgrade selection

option interface to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing transaction services to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing bill by account functionality for the network. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing some amount of free networking or information service to entice the user to use the other ambient services. In some embodiments, the aforementioned ambient service is at least partially implemented with device based service activity control or control assistance. In some embodiments, the aforementioned ambient service is at least partially implemented by gateways, routers or switches in the network that are programmed according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account.

[0477] In some embodiments, activation is accomplished at least in part with a temporary service account in a manner that is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary service account is replaced at a later point in time by permanent service account subset in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary service account settings (e.g., including the service profile settings and/or the service plan settings) are pre-programmed into the device along with a temporary or permanent credentials set during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming for the network is performed via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, the device is suspended once it is activated but before the user is using it, and then resumed before or commensurate with the point in time that the user begins to use it. In some embodiments, some subset of the temporary service account is recycled once it is replaced, if the temporary service account is not used after some period of time, if the temporary service account is not upgraded to a permanent service account after some period of time, or if the activation is revoked from the device for some other reason. In some embodiments, more than one device is assigned to the

same temporary service account. In some embodiments, a network accepts more than one device on the same temporary service account. In some embodiments, a device includes or is associated with two or more temporary service accounts, in which at least a subset of the temporary service account elements are different, so that if one account is already being used to access the network then one or more reserve accounts can be drawn upon to gain access to the network. In some embodiments, the temporary service account is associated with a temporary credentials set. In some embodiments, the temporary service account is associated with a permanent credentials set.

[0478] In some embodiments, un-activated devices are detected by the network routing equipment (e.g., service gateways or routers in hierarchical networks or base stations with embedded gateways in flat networks) and the device routing is programmed to re-direct un-activated devices to an activation server network destination. For example, the activation server can first inspect the information associated with the device to determine if the device belongs to the list of devices, device types or device groups that the network is programmed to provide access to. For example, the information used to determine this can include device type, service provider, phone number, device ID, SIM ID or configuration, secure information used to qualify the device, IP address, MAC address, user, user group, VSP, OEM, device distributor, service distributor (master agent), service processor presence or configuration, presence or configuration of other software or hardware. There can also be some activation definition information embedded in the credentials, or associated with some portion of the credentials, or programmed additionally on the device that informs the activation server as to the service profile and/or service plan and/or service account that should be established for the device. If activation information (the service profile, service plan and/or service account information) is found through association with the device credentials (e.g., device ID, phone number, IP address, MAC address, SIM or other security credentials) rather than being read directly from information embedded in the device or device credentials, then the pertinent aspects of the credentials can be used as a cross reference to look up the service plan and/or service profile information stored in a database networked to or within the activation server. The activation information can include information to define a wide variety of service plans and service profiles that when properly implemented on the network functions, and perhaps device if necessary, can provide for a wide range of service activity policies, service billing policies, transaction billing policies and service account types that can be associated with the device over the air or over the network.

[0479] In some embodiments, once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server initiates the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up may be permanent or temporary. In some embodiments, the activation process described above is completed perhaps before the user has entered some or all of the user information necessary to set up a permanent service account, and, in these cases, a temporary service account can be set up. In some cases, the activation process can be completed in the background before the user has completed an attempt to access the network and the service profile can be set up to provide ambient services to a temporary service account. In some embodiments, the user is required to enter the information required to establish a permanent service account prior to gaining full use of the device, either on the device, on a computer or in the store, so that by the time the user begins using the device the above activation embodiments can provide for ambient services activation with permanent account status so that the user can purchase a service upgrade or any transaction without entering any more account information.

[0480] In some embodiments, a device status is changed from a temporary service account to a permanent service account. If the device is activated with a temporary service account, and the user information is available to set up a permanent account, then if the billing system rules and interfaces allow for such, the user information can be changed from the mock information to the actual user information while maintaining the same account identifiers in the billing system. If the billing system will not allow for such, then the user information can be used to establish a new account, the device credentials can be re-associated with the new account, in some cases, after modifying one or more of the device credential parameters, and the network functions can be re-programmed as required, and, in some cases, the device can be re-programmed as required to accommodate the new permanent account.

[0481] In some embodiments, code on the device pulls a temporary or permanent set of credentials. When the credentials are pulled, the network associates the device with an ambient service profile according to one or more of the following: embedded device information identifying device type, service owner (e.g., VSP), user group, or user, or device ID is cross referenced to a database that is populated some time from manufacturing time to post sale where the database provides information identifying device type, service owner (e.g., VSP), user group, or user. The device is then re-directed accordingly (e.g., for device based this is a matter of setting the policies or loading the software for the service processor, for the network based approach this is a matter of populating the routing tables and service profile). For example, credentials can be re-cycled after a period of time, and/or some portion of the credentials can be redundant with other devices. For example, this is essentially a dynamic service for (temporarily) assigning device credentials, and the duration of the temporary credential validity for that device ID can be time limited to give the user time to activate a real account or a free trial, session limited, or a longer duration of time that is perhaps refreshed each time the device logs on. For example, the device could also already have permanent or temporary credentials but not have a service account. The above process can be used to assign a temporary or permanent service account as well. Once the service account is assigned and the appropriate service profile is propagated to the network elements, the device can then be directed to or use the appropriate activation profile service activities or the appropriate ambient service activities.

[0482] In some embodiments, the device is activated in the background in a manner that is virtually transparent to the user. For example, at some point in the distribution channel, the device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device connects to the network and the gateways or routers re-direct the device to an activation server, as discussed above. As also described herein, the activation server either derives information from the device that informs the server what service the device should be activated with, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server causes all the necessary network settings and billing database entries to be

configured/programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. For example, the provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

[0483] In some embodiments, background activation is performed using the aforementioned activate/suspend process. At some point in the distribution channel, the device is programmed to seek to resume service as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device attempts to connect to the network and the gateways or routers re-direct the device to an activation server as described herein. As also described herein, the activation server either derives information from the device that informs the server that the device is ready to resume service, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the server is aware of this information, it sends a message to resume service to the billing system, or other network function that controls the suspend/resume function, and the service is resumed.

[0484] In some embodiments, background activation is performed as described below. The service processor and the credentials are pre-programmed during the manufacturing or distribution process to provide the desired service profile support and/or billing profile support for the desired initial ambient service. As described herein, this programming can be accomplished with dedicated apparatus at the manufacturer or distribution depot. Furthermore, the party responsible for defining the service (e.g., typically the central provider, OEM, VSP, distributor or master agent) can network into the service processor programming apparatus to control service processor and/or credential programming for all or a subset or group of the devices or device types locally available. The service processor enabled device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. In some

embodiments, the activation server is the access control server previously discussed or the access control server can act in concert with another server that performs the activation function. When the pre-programmed event is triggered, the device connects to the network and the gateways or routers re-direct the device to the activation server. As also described herein, the activation server can communicate with the service processor to verify the service processor security credentials, agents and configuration.

[0485] In some embodiments, if the activation server determines that the pre-programmed settings stored in the service processor need to be modified to provide the latest version of the desired service, or if the service processor agent software needs to be updated, then this can be accomplished prior to completing the activation process. Once the service processor configuration and settings are confirmed, the activation server causes the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. Given that the service processor can perform some or much of the service activity control or control assistance, the service control options are generally larger than without the service processor, and there can be less configuration to perform for other networking equipment to complete the provisioning and activation process. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

[0486] In some embodiments, pre-programming and pre-activation of devices with temporary credentials and a temporary service account are used to ship devices that are pre-activated. Given that the credentials are temporary and can be recycled when the permanent credentials are assigned, concerns about using up too many pre-assigned credentials are reduced. In embodiments in which a portion of credentials elements can be used for multiple devices, this concern is further reduced. If there is a concern about too many activated devices being assigned that are not actually active and generating service revenue, then the suspend/resume process discussed herein can be employed. In some embodiments, the temporary credentials and/or temporary account can be replaced with permanent credentials and/or account assignments at any time as follows. When a pre-programmed event in the device is triggered, then the device initiates a program that seeks the aforementioned activation server or another server that has the

capability of fulfilling the device request to exchange the temporary credentials for permanent credentials and/or exchange the temporary account for a permanent account. The event that triggers the credential exchange can be the same or different than the event that triggers the service account exchange. The service account exchange can typically be triggered by the point in time that the user enters account information.

[0487] In some embodiments, the aforementioned ambient service is partly implemented with a combination of the techniques for pre-provisioning during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy provisioning capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are pre-programmed as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the provisioning credential elements are not all pre-programmed before the device ships, but a subset of the credential elements are programmed using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service activity control settings for the gateways, routers or switches that will result in the desired ambient services activity controls.

[0488] In some embodiments, the aforementioned ambient service is implemented with a combination of the techniques for pre-activation during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy control capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are programmed to recognize the pre-activated device credentials as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the device activation profile and/or service account are not pre-programmed in the network and/or the device before the device ships but the activation profile and/or service account are programmed

using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service profile activity control settings for the gateways, routers or switches that results in the desired ambient services activity controls.

[0489] In some embodiment, a VSP capability is enabled by providing a secure network connection to the service policy settings tools that define the device pre-provisioning settings, the device pre-activation service profile settings, the network equipment service activity control policy settings (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage), and the network billing system database. By providing server tools that enable all these settings to be controlled (or perhaps only observed in the case of the billing system) by a secure workstation or secure website interface that networks into the equipment that programs the settings, and providing for a secure partitioning of the devices that can be controlled by a given secure workstation or secure website interface, a central provider can provide VSP services to multiple entities who all have different device and service plan combinations that they desire different flavors of ambient services for. These techniques can also be extended beyond ambient to any device/service profile/service plan combo the VSP desires to create. In some embodiments, the networking equipment is implemented to secure device service group domains in which the service policies for a group of devices can be controlled. In some embodiments, the pre-provisioning and pre-activation techniques are substituted with the over the air activation server techniques discussed herein, and a secure device group partition capability is provided in the activation server as well so that the activation server device group partition control capabilities can be added to the secure device group partition control capabilities of the network gateways, routers and/or switches, the device programming tools and the billing system to form a VSP partition solution for over the air activation of various device/service plan combinations. In some embodiments, the device groups are relatively small so that beta trials of arbitrarily large or small size can be designed and implemented by defining a service control group as described above, and after fine tuning and perfecting the beta trial settings the device group can be expanded to publish the automated provisioning and activation service settings to a larger user or device group for production services.

[0490] In some embodiments, device based service activity control assistance (e.g., based on the various service processor embodiments described herein) is combined with simplified provisioning techniques described herein so that service processor enabled devices can be shipped with pre-provisioned credentials (temporary or permanent) or can obtain credentials in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain credentials and provisioning apparatus described elsewhere provide various approaches for provisioning pre-provisioned service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various approaches for over the air or over the network simplified post-sale provisioning for service processor enabled devices. For example, these embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

[0491] In some embodiments, provisioning includes provisioning partial device credentials that include, for example, a secure certificate that is used to authorize full credential provisioning and/or activation by performing a process for a later look-up/validation of the full device credentials. For example, the look-up/validation of the full device credentials can be performed by a gateway, router or similar network device that re-directs to a provisioning server and/or activation server or other network components that either: (1) recognizes the partial credentials that serve as a reference to direct the device communication to a specific provisioning/activation server determined from the partial credentials; or (2) does not recognize the partial credentials, and directs the device communication to a less specific provisioning/activation server that is not necessarily associated with a reference to the partial credentials.

[0492] In some embodiments, if the partial device credentials (e.g., temporary or permanent credentials) are being used for provisioning, then the partial credentials are read (e.g., and/or other credentials can be looked up based on the partial credentials as described above). The device is authorized if the proper credentials and/or secure certificate is present. The device credential provisioning is then completed (e.g., using activation server commands or settings to a

device based software and/or hardware element), and the credentials are, in some cases, also communicated to the various network equipment elements.

[0493] In some embodiments, if the partial device credentials are being used for activation, then partial or full device credential provisioning is performed, such as described above. A service account (e.g., temporary or permanent service account) is created or looked up based on the partial device credentials (e.g., a user account associated with the device through embedded partial or full credentials or a look up process, or based on a dynamically created/assigned temporary account associated with the device through embedded partial or full credentials). An initial service profile and, in some cases, an initial service plan (e.g., service control policy settings including a billing profile) are determined from embedded information and/or using a look up process (e.g., based on the device type and/or partial or full device credentials). The device is then programmed to enable access with the service profile and plan, and, in some cases, the various network components/elements are programmed to enable the service profile and plan, and, in some cases, proper entries in the billing system are made or confirmed, and the device credentials are, thus, activated for service.

[0494] In some embodiments, the above described provisioning and/or activation processes are performed with the provisioning server(s) and/or activation server(s) in the background with reduced, minimal or no user input required, for example, after the device is sold to the user and the user turns on the device so that by the time the user attempts to access the service using the device, the provisioning and/or activation process is already completed.

[0495] In some embodiments, device based service activity control assistance (e.g., based on the service processor embodiments) is combined with simplified activation techniques described herein so that service processor enabled devices can be shipped with pre-activated accounts (temporary or permanent), or can obtain activated account status in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain activation and provisioning apparatus described elsewhere provide various approaches for pre-activated service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various

approaches for over the air or over the network simplified post-sale account activation for service processor enabled devices. These embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

[0496] As discussed herein, in some embodiments for activation, the network AAA (or other network function) either recognizes one or more aspects of a pre-activated device credentials and routes the pre-activated device communication to an activation server that is appropriate for that device (routing information either derived through look up of the credential aspect or by obtaining the required information directly from the credential itself), or the AAA (or other network function) does not recognize the credentials and routes the device communication to an activation server for unrecognized device credentials. In either case, in some embodiments, one or more of the credential aspects can then be used to perform a secondary determination of what provisioning and/or activation sequence to perform in association with the device, or which activation server sequence the device should be directed to. For example, one or more device credential aspects can be read and used as a cross-reference to determine a routing for the device communication (or the information required for routing can be in the device credential information itself) so that the device can be routed to the appropriate activation server sequence.

[0497] In some embodiments, an activation server sequence can be determined at least in part by using a browser server or a portal (e.g., http server, https server, WAP server or another standard or custom protocol server for a browser, embedded or automated browser or a portal client in the device). In some embodiments, the browser server is an http or https server. The pre-activated device communication can be routed to the https server in a manner similar to that described above, and the server can read the information embedded in the https communication to determine the device credential information required to initiate the correct provisioning completion and/or activation sequences. For example, the https header information, tokens, cookies or other secure information communicated over https from a secure embedded client on the device (or user) can either provide the activation server with the information required to perform the cross-reference to an appropriate provisioning and/or activation sequence, or the https embedded information or the embedded client (or user) information can instruct the

activation server on which services the device is to be provisioned and/or activated on and any necessary device or user information (e.g., device owner and/or billing information) can be exchanged, or the device might be provisioned and/or activated first on a free ambient service with temporary or permanent credentials or account.

[0498] In some embodiments, the service processor can be combined with the pre-provisioning and pre-activation techniques described above to create an ambient service solution that will work on roaming networks in which the central provider or VSP has no control or minimal control over the network elements. For example, the device includes a service processor pre-programmed for ambient service activity control as discussed herein, and the device credentials and other settings are pre-provisioned and pre-activated for the central provider network, all of which is described in numerous embodiments disclosed herein. Provided that the service provider has a roaming agreement with other service providers, or provided that the device may gain access to the roaming network, when the device is roaming it will be capable of ambient connectivity with bill by account functionality and all the other features of ambient. Furthermore, as also discussed herein, the ambient service activity control policies can be different for different roaming networks to accommodate the varying network costs and performance. Also, for example, it would be permissible to sign up for initial services or additional upgrade services with the central provider while roaming on the roaming partner network. One of ordinary skill in the art will appreciate that this also allows for creating a VSP or MVNO for the purpose of creating a clearing house for central provider service activations according to geography or user choice. By using a global multi-mode modem module, and maintaining service agreements with a multitude of carriers, the MVNO or VSP can provide consistent ambient services across multiple carriers and multiple geographies while still maintaining a good degree of cost control. Using bill by account capabilities, it is also possible to have an activation agreement where a roaming service provider agrees to refund the cost of ambient roaming. From the ambient service platform, the VSP or MVNO can then provide service purchase options to the user based on the carrier networks available to the device, or the VSP or MVNO can broker the user off to any of the carriers by activating the device onto the carriers main central provider service.

[0499] Accordingly, these embodiments provide flexible capabilities for activating a device or group of devices with a broad range of service profiles and service plans by simply programming the device with the proper credentials at some time during manufacturing or distribution, or simply programming a database associated with the network so that a portion of the device credentials can be used to look up the desired service profile and service plan. For example, various activation embodiments described herein are highly convenient for the end user and need not, in many cases, involve any human intervention.

[0500] The service processor 115, service controller 122, policy implementation and/or profile implementation and various embodiments disclosed herein are applicable to conventional communication products as well as machine to machine applications. For example, if the machine to machine device includes a service processor 115 with an activated account, then the service profile settings can be optimized for machine communications to provide only the limited access required to support the particular machine to machine application. This allows for cost optimized access services and prevents the machine to machine device or access modem from being misappropriated and used for some other service access than that intended. For example, by programming the machine to machine communications device at time of manufacture or during distribution with credentials or partial credentials that provide for automated provisioning and activation as described herein, the device can be automatically provisioned and activated on the service network with a service account when deployed, thus eliminating the need for costly or time consuming human intervention. The various embodiments that make it simpler to design, manufacture, test and deploy devices may also be equally applied to machine to machine devices. These embodiments include the service processor 115 developers kit and the automated provisioning and activation management tools among others. Also, the service analysis and test tools and the virtual service provider embodiments can also be applied to machine to machine applications.

Verifiable Device Assisted Services For Intermediate Networking Devices

[0501] It should be appreciated that the various service monitoring, notification, control and billing embodiments disclosed herein can also be applied to intermediate networking device applications.

[0502] In some embodiments, an intermediate networking device is a communications device in which the service processor 115 is configured at least in part to allow the intermediate networking device to act as a service intermediary or intermediate connection between the network and one or more end point devices (e.g., communications devices). In addition, a service controller 122 or other suitable network functions can be employed to assist with the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein. In some embodiments, an intermediate networking device does this by implementing the service policies required for assisting service usage control of the intermediate networking device and connecting the network to provide services to one or more end point devices that are connected to the intermediate networking device. In some embodiments, the intermediate networking device also monitors the service use activities of the intermediate networking device and/or the end point devices connected to the intermediate networking device. In some embodiments, the intermediate networking device and/or end point device service usage is verified to ensure that the service usage is within the expected ranges for the policies that are implemented. In some embodiments, the intermediate networking device connects with the network using one modem technology and connects with the end point devices using one or more additional technologies. In some embodiments, an intermediate networking device connects the end point devices to the network by passing, bridging, forwarding, routing, traffic shaping or otherwise allowing the end point devices to communicate with the network. Example intermediate networking device embodiments include a Wi-Fi to WWAN (e.g., 2G, 3G, 4G or other wireless wide area networking access technology) bridge or router device, a Wi-Fi to DSL, cable or fiber gateway device, a WWAN to DSL or Cable femto cell device, a WWAN and Wi-Fi to DSL, Cable or fiber back-hauled femto cell device, a WWAN to WWAN router device, a WWAN to WLAN, WPAN or LAN bridge, router or gateway device, or a WWAN back up connection device for an enterprise router.

[0503] An intermediate networking device can also be provided in some embodiments by including a bridging, forwarding or routing function between two modems in a communications enabled device that connects to the network. For example, an intermediate networking device configuration can be a cell phone, smart phone, mobile internet device or any other mobile device that includes a WWAN modem and a Wi-Fi, WLAN, WPAN or LAN connection that can be used to connect to other end point devices. For example, the mobile device WWAN modem

can connect to the network, a service processor 115 can be included on the device processor to assist monitoring, controlling and billing for services between the WWAN network and end point devices connected to a Wi-Fi modem. In addition, a service controller 122 or other suitable network functions can be employed to assist with verifiable service usage monitoring, control and verification as disclosed in numerous embodiments disclosed throughout herein. In some embodiments, the Wi-Fi modem can be configured in access point mode or in ad hoc mode to communicate with other end point devices in the area covered by the mobile device WLAN modem. In this manner, a service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein.

[0504] Another example embodiment is a notebook or sub-notebook computer with a WWAN modem and a Wi-Fi, Ethernet, Firewire, Bluetooth, near field or Zigbee modem in which the notebook processor has a service processor 115 running on the notebook processor and the service processor 115 is used to assist monitoring, control and billing for services communicated between the WWAN network and end point devices connected to the notebook or sub-notebook WLAN, LAN or WPAN. Another example embodiment is a Wi-Fi hot spot with a service processor 115 capability. Another example embodiment is a WWAN back up modem in an access network router where the back up modem connection to the WWAN network is used when the main wired network connection goes down, and a router processor or a WWAN back up modem processor runs a service processor 115 to assist monitoring, controlling and billing for services between the WWAN network and the access router (e.g., the service provider may only wish to enable a connection when the main wired network is down to ensure that the WWAN modem is not used for everyday access). In this manner, a service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein.

[0505] Another example embodiment is a two-way home gateway configured to perform various functions such as reading power consumption of the home and/or components in the home, providing WLAN, WPAN or LAN connectivity for such components or to the power meters/controllers attached to such components, providing a WWAN or WAN connection to a

network that reads, records, monitors and/or controls the home and/or component power consumption, and possibly to provide other wide area network services for other devices in the home such as computers or entertainment electronics in a similar manner to the WWAN, DSL, cable and fiber gateway embodiments. The WLAN, WPAN connections can be made with one or more of Wi-Fi, Zigbee, Bluetooth, NFC or any other suitable wireless modem technology, and any desired wired LAN connections may be made with one or more of Ethernet, USB, Firewire, data over cable, data over power line or any other suitable wired modem technology. The WWAN connections can be made with one or more of 2G (e.g. CDMA 1xRT, GPRS), 3G (e.g. WCDMA UMTS/HSPA/non-MIMO HSPA+, CDMA EVDOa/B, 802.16d/e WiMax), 4G (e.g. LTE, MIMO HSPA+, MIMO 802.16m WiMax) or any other suitable modem technologies and the wired WAN connections may be made with one or more of DSL, Cable, fiber or any other wired modem technology. A service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments disclosed throughout herein.

[0506] In some embodiments, an intermediate networking device can be used to connect one end point device to a network and assist in implementing service policies, or an intermediate networking device can connect multiple end point devices to one or more networks and assist in implementing service policies. In some embodiments, an intermediate networking device can be associated with one service profile, one service plan or one service account, or an intermediate networking device can be associated with multiple service profiles, multiple service plans or multiple service accounts. In some embodiments, end point devices connected to an intermediate networking device can have service usage policies implemented in aggregate for all end point devices, or service policies can be implemented differentially for different end point devices.

[0507] In some embodiments, an intermediate networking device can have a network connection associated with a single account and manage QOS between end point devices under one umbrella service profile or collection of profiles. In some embodiments, an intermediate networking device can treat all connected end point devices equally from a service sharing or QOS perspective so that, for example, service usage is based on end point device demand and/or contention. In some embodiments, an intermediate networking device differentiates service

QOS between different end point devices based on end point device service demand or service usage patterns, EDP device type or device group, end point device user or user group, end point device service account status or service plan status, or end point device application type, and/or traffic type or service type.

[0508] As discussed herein, the service processor 115 function assisting intermediate networking device implementation can be included on the intermediate networking device, can be included in part on the intermediate networking device and one or more end point devices, or can be implemented mainly or entirely on one or more end point devices.

[0509] In some embodiments, an intermediate networking device can be constructed in which end point devices connect to the intermediate networking device and gain access services to a WWAN network through a WWAN/Wi-Fi enabled intermediate networking device that is supplied with services associated with a single account and service profile. The intermediate networking device service processor 115 can assist in monitoring, control and billing for WWAN service usage for all end point devices in the area covered by the intermediate networking device Wi-Fi link. In some embodiments, end point devices receive service on first come first serve basis with no differentiation. In some embodiments, end point devices receive fair distribution of services so that if one end point device is using more significantly more service than the other end point devices, or is demanding more service than the intermediate networking device service profile settings provide for a single end point device (e.g., “bandwidth hogging”), then the high demand end point device is throttled and the other end point devices are not. In some embodiments, end point devices receive hierarchical distribution of services based on one or more of service type, device type, user type, and/or account status. In some embodiments, an intermediate networking device can provide for a large or unlimited number of end point devices to connect to the network and simply control aggregate service usage parameters for the intermediate networking device WWAN connection. In some embodiments, the intermediate networking device limits the number of end point devices that are allowed to connect to the WWAN network according the end point device count limits programmed in the service processor 115 service profile settings in the intermediate networking device. In some embodiments, end point device traffic can be identified by various end point device credential aspects including, for example, by Wi-Fi ID, MAC ID, IP address, user ID, LAN tag, end point

device agent credentials, and/or browser token or cookie. In some embodiments, the intermediate networking device service account can be billed for overall service usage and/or by number of end point device connections allowed or experienced. In some embodiments, as the intermediate networking device user or owner signs up for a higher end point device connection count, one or more aspects of the service usage policy implementation and/or profile implementations in the service processor 115 profile settings can be increased.

[0510] The various verification techniques described herein can also be applied to the intermediate networking device and extended to multiple end point devices. For example, network based service usage measures for verification can be applied to the intermediate networking device just as if the intermediate networking device were an end point device. For example, network based service usage measures (e.g., IPDR information) can be used to perform network verification checks to ensure that intermediate networking device service usage is within acceptable ranges based on intermediate networking device policy settings as similarly described with respect to various device embodiments. In some embodiments, in the event intermediate networking device service usage is outside the policy limits set for the intermediate networking device service processor 115, a notification can be sent to the intermediate networking device main account owner. The main intermediate networking device account owner can also be required to acknowledge the notification. The notification can also be sent to one or more other users of the intermediate networking device connection, including possibly all users. Other actions that can be taken if the network based intermediate networking device service usage measure does not match the policy limits set on the service processor 115 include notify the user, notify the user and require acknowledgement, bill the user for service overage, suspend the end point device, quarantine the end point device, SPAN the end point device, and/or alert network manager or alert an automated network troubleshooting function. In some embodiments, a device based usage measure can be verified against a network based service usage measure. It will now be apparent that the various service processor 115 verification embodiments, service controller 122 verification embodiments, network verification embodiments, authentication embodiments, and tamper prevention or detection embodiments, such as those shown in and described with respect to FIGS. 22A, 22B, 23, 26A-26H, 27A-27P and 28A-28E, can be applied to intermediate networking device applications and embodiments.

[0511] In some embodiments, it is desirable to match up individual end point device or user intermediate networking device service usage with other service usage measures. For example, the individual end point device service usage measures logged or reported from the end point devices and/or the intermediate networking device can be aggregated to form a total intermediate networking device usage measure that is compared to an aggregate intermediate networking device usage measure logged or reported in the network. In some embodiments, if these measures do not match, then an error condition results and an action is taken. In some embodiments, the aggregate intermediate networking device service usage measure is compared to the aggregate network based service usage measure and as long as these two measures are within an acceptable tolerance, then the intermediate networking device service usage measures are trusted and can be used for deeper intermediate networking device and end point device usage measures for service control and/or billing than may be possible in the network. In such embodiments, the individual end point device service usage measures gained from the intermediate networking device or end point device can be used to verify end point device service usage versus service policy allowances. In some embodiments, end point device service usage measures are compared with intermediate networking device measures for the same end point devices.

[0512] In some embodiments, the IPDR records for one or more networks can include individual end point device service usage information. This is the case for example when the IPDRs include information broken down by end point device credential, such as IP address or other end point device credential. In such cases, intermediate networking device embodiments can be employed in which the individual end point device service usage information measured in the network can be compared with the service usage policy allowances or limits for the end point device. Also, in some embodiments, the individual end point device service usage measures from an end point device service usage monitor and/or an intermediate networking device service usage monitor can be compared with the network based service usage information to verify an end point device and/or an intermediate networking device service usage monitor is operating properly.

[0513] As similarly described with respect to end point device embodiments with no intermediate networking device between the end point device and the network, in some

intermediate networking device embodiments, service usage and service usage monitor reports can be periodically verified by performing a SPAN function on the traffic for an intermediate networking device. The SPAN traffic can be analyzed in a real-time manner or in a non-real-time manner in the network and the results can be compared with the intermediate networking device or end point device service policies or service usage measures.

[0514] The synchronized device notification and acknowledgement embodiments can also be employed in the case in which one service account is applied to the intermediate networking device. The service usage counters in the intermediate networking device can be synchronized or updated with the network based measures and the differences between the two may be minimized. The service usage notification can be sent to one or more of the end point devices connected to the intermediate networking device. For example, the notification can be sent to the intermediate networking device manager or service owner, all end point devices or the most active end point devices.

[0515] Similarly, user preference feedback can be collected from one or more of the service users connected to the intermediate networking device. In some embodiments, user preferences or user service selections or service settings are collected from one user or a subset of end point devices used by the service subscriber. In some embodiments, more than one service user can provide preference information or service settings even if there is only one user account. In some embodiments, there are multiple service subscribers each providing preferences. In some embodiments, as similarly described with respect to various device embodiments, user preferences can be used set service control policies that provide the user with their selected balance of cost and service capability in a manner that meets network neutrality requirements. Similarly, in some embodiments, the service monitoring and customer resource management information collected on the intermediate networking device or end point devices can be filtered according to user privacy preferences to maintain the level of user privacy selected by the user.

[0516] Adaptive intermediate networking device policy implementation can also be performed in the intermediate networking device service processor 115 embodiments, as similarly described with respect to various device embodiments. In some embodiments, the

service policy implementation for the intermediate networking device can be adapted by the service processor 115 agents (e.g., policy control agent 1692 working to control the settings in policy implementation agent 1690, and/or another service processor agent or function) to achieve a higher level service usage goal. In some embodiments, the usage goals or adaptation can be based on aggregate end point device usage for the intermediate networking device network services, and in some embodiments, the higher level usage goals or adaptation can apply to one or more individual end point devices.

[0517] In some embodiments, even though there is one intermediate networking device account, there can be multiple options for multi-end point device or multi-user operation in which the number of end point devices, number of users or service capabilities for some of the end point devices or users are selectable. These parameters are accommodated by an intermediate networking device service profile that includes the service capabilities that are to be delivered to a multitude of end point devices or users. In some cases, some end point devices or users have a different profile within the intermediate networking device service processor 115 with differentiated capabilities as compared to the intermediate networking device service processor 115 profile for other end point devices or users. This is the case for some of the examples provided herein. These multi-end point device or multi-user service profiles in the intermediate networking device service processor 115 can share services equally or can allow more capable access services to some end point devices or users than others. In some embodiments, a service profile implemented by the intermediate networking device service processor 115 for one end point device or user is different than that in the service profile implemented by the service processor 115 for another end point device or user (e.g., providing differentiated service profile implementations by end point devices and/or users). End point devices can be uniquely identified for purposes involving implementation of different service profiles in the intermediate networking device service processor 115 agents (e.g., depending on the embodiment, service monitor agent 1696, policy implementation agent 1690, policy control agent 1692, application interface agent 1693 and/or other service processor agents or functions) based on a number of parameters, such as IP address, local area network address (e.g., Wi-Fi address), MAC address end point device ID, user ID, and/or end point device application layer tag. This allows for independent service usage monitoring and control for different end point devices or users.

[0518] In some embodiments, an intermediate networking device also bridges services to end point devices or users that have individually managed service profiles, service plans or service accounts. As discussed herein, individual end point device service policy implementation and/or service profile implementation can be accomplished by classifying end point device service usage according to an end point device identifier so that service monitoring, control assistance and reporting may be differentiated between one or more end point devices. These end point device identifiers can then be associated with a different service plan or account in the service processor 115 and/or billing system 123. The end point device or user specific service usage monitoring, reporting, notification and control assistance can be accomplished by running one or more profiles for each end point device or each user.

[0519] It will now be apparent that billing can also be implemented with a single account encompassing service usage for all users or end point devices connected to an intermediate networking device, or for individual users, end point devices, user groups or end point device groups connected to an intermediate networking device. As similarly described with respect to the service profile, this is accomplished by associating service usage events and associated billing events with an end point device identifier, user identifier, end point device group identifier, and/or user group identifier.

[0520] In some embodiments, end point devices or users connect to more than one intermediate networking device with the same service account, service plan or service profile. In some embodiments, the intermediate networking device requires an authentication sequence for the end point device or user before allowing connection to the network through the intermediate networking device. This authentication sequence can involve the end point device communicating an active account or admission credential with the intermediate networking device. The intermediate networking device can compare the credential with a local database or may query a database in the network to admit the end point device to the intermediate networking device network connection. In either case, provided the user credential or network authorization process is passed, the service processor 115 service profile settings for the end point device are applied and service is then established as discussed herein. In these cases, the verification can be accomplished as described herein. In some embodiments, even if the end point device does not have a service processor 115, provided that the intermediate networking

device service policy implementations and/or service profile implementations are verified as described herein, then the intermediate networking device will accurately assist in control and reporting of service usage for the different end point devices or users, and the appropriate service policy controls and/or billing can be maintained.

[0521] In some embodiments, when the end point device attempts connection to the intermediate networking device, if the user or end point device does not already have an active account or logon credential that the intermediate networking device recognizes, then the intermediate networking device can offer the end point device or user a service sign up experience. This experience can be implemented in a number of ways, including a website, WAP site, portal, download of agent software, and other methods. For example, an automated recognition of new devices can redirect unauthorized end point devices to browse into a website, WAP site, or portal site located on the intermediate networking device or in the network. If the site is located on the intermediate networking device, it can be cached and refreshed at a time of day when the network is not overly busy. Once on the site, the user or end point device selects the plan choice they desire, inputs account information and, in some embodiments, downloads device agent software to aid in network service policy implementation and/or profile implementation with the intermediate networking device. Once the user signs up, the information is logged into the network data base, the service account is established and the intermediate networking device service profile for that user or end point device is activated and the user can begin using the service.

[0522] In some embodiments, a website, WAP site, or portal site located in the intermediate networking device can be used to provide the end point device user with a service usage monitor interface and a service purchase interface for cases in which the end point device does not possess any special software to allow it to display a more specialized service usage monitor function for information received from the intermediate networking device or network service usage counters. The service usage monitor for the intermediate networking device can be synchronized, as similarly described with respect to various device embodiments. In some embodiments, the service usage notification system can also display cost data from a usage to cost look-up function. In some embodiments, the service usage notification system can display projected service usage or projected cost, as similarly described with respect to various device

embodiments. The service usage monitor to drive these service notification embodiments can be located on one or more of the end point device, the intermediate networking device or the network.

[0523] In some embodiments, if multiple accounts are serviced by one or more intermediate networking devices, verification can be performed on the service controls for the end point device or user service usage. As will now be apparent, just as with the intermediate networking device, the end point device or user service usage comparison with usage policy settings can be verified in the ways described herein. If the usage is found to be out of policy, then any of the out of policy actions described herein can be performed, including, for example, notify the end user, notify and require acknowledgement, bill for overage, suspend, quarantine, SPAN, and/or flag to network manager or network error handling function. For example, the verification methods shown in and described with respect to FIGS. 22A, 22B, 23, 26A-26H, 27A-27P and 28A-28E can be applied for the embodiments where intermediate networking devices have multiple account, multiple service plan, multiple service profile, multiple end point device, and/or multiple user capabilities.

[0524] It will be apparent that the various embodiments described herein for automated provisioning and activation also can similarly be applied to the intermediate networking device embodiments. It will also be apparent that the various virtual service provider embodiments can similarly be applied to the intermediate networking device embodiments.

[0525] Ambient services can be employed on the intermediate networking device and the ambient services can thus be provided to the end point devices. It will be apparent that the ambient service profile embodiments disclosed herein can similarly be applied to the intermediate networking device, and then the intermediate networking device can supply those ambient services to end point devices connected to the intermediate networking device. It will also be apparent that the intermediate networking device can provide an ambient service profile as described herein to end point devices or users that have not yet signed up for service, while providing other paid for service profiles to end point devices or users that have signed up for service.

[0526] Bill by account embodiments can similarly be applied to the intermediate networking device embodiments. For example, bill by account can be used in embodiments in which all end point devices or users are connected to the intermediate networking device under one account, or to embodiments in which some end point devices or users are accounted for separately with different service accounts, service plans or service profiles. In either case, it will be apparent that using one or more of the end point device or user identification credential aspects discussed herein can be used in a bill by account profile to account for any end point device or service activity. In such embodiments, billing event reports for those activities that include the end point device or user identifiers can also be provided for billing mediation and reconciliation down to the individual end point device or user level. For example, this allows for very deep service monitoring and billing capabilities with intermediate networking devices.

[0527] The intermediate networking device embodiments described above also have uses in machine to machine applications. It will be apparent that if the end point device includes the correct credentials to gain access to an existing account, or to allow an automated provisioning and activation account to be established, then the end point device can be connected to the network through the intermediate networking device without human intervention. Furthermore, the service profile that is established with the end point device for machine to machine communications can be set up to provide the access required to support the machine to machine application allowing for low cost access services and preventing the end point device from being misused for some service other than that intended. For example, the verification techniques and embodiments disclosed herein can similarly be applied to such machine to machine applications.

[0528] It will be apparent that the identifiers discussed above for bill by account mediation with accounting down to the individual end point device or user level can be combined with a billing mediation server in the network that accepts intermediate networking device billing events with end point device identification or user identification indexed billing, performs the necessary bill by account mediation functions, formats the billing events into the format used by the billing system, and transmits the mediated billing information to the billing system 123.

[0529] In some embodiments, the intermediate networking device service processor 115 functionality can be split. The division ranges from some or all of the service processor 115 on the device to some or all of the service processor 115 on the intermediate networking device.

[0530] In some embodiments, all of the service processor 115 is on the intermediate networking device. The end point device does not participate in service processor 115 functions and has no service processor 115 interface software. In some embodiments, the end point device has small subset of service processor 115 capabilities, including, for example, a service notification UI or a logon client with credentials. In some embodiments, service monitoring is implemented on the end point device or on both the end point device and in the intermediate networking device. In some embodiments, the end point device has additional service processor 115 capabilities including, for example, application layer tagging that associates application layer activity with service processor 115 service monitoring or service policy implementation and/or service profile implementation information. This can be accomplished by a range of techniques, for example, transmitting the application tagging information disclosed elsewhere to the intermediate networking device service processor 115 so that the policy implementation may be accomplished with knowledge of the application layer information. Another example involves assigning IP addresses in the intermediate networking device networking stack to the end point devices so that different types of end point device traffic can be routed into service processor 115 traffic shaping queues, each queue having a policy profile implementation engine, and application layer tagging information or similar traffic identifying information is used to determine which policy implementation engine the traffic should be routed to in order to accomplish the desired traffic shaping for the traffic type, application type, service type, and/or content type. In some embodiments, the traffic control policy is implemented on the end point device either with an application layer traffic controller, or by implementing more of the service processor 115 functionality, as similarly described with respect to various device embodiments. In the end point device service functionality example, most or all of the service processor 115 functionality is implemented on the end point device and the intermediate networking device functionality can be reduced to a bridging, forwarding or routing function between the end point devices and the network that performs little or no service control, monitoring and/or billing functions. For example, the service usage monitoring agents can also be provided on the end point device to aid in verification.

[0531] In embodiments in which the end point device requires agent software, the software can be loaded at time of manufacture or during distribution, loaded later, and/or made available for download through the intermediate networking device. In the case in which the end point device agent SW is downloaded through the end point device, there can be locally cached copies of the SW for one or more OS variants stored in a cache on the intermediate networking device, with the cache being updated over the network at convenient or conducive times, or the software can be downloaded live over the network when it is needed by the end point device. Logging the service usage to download this software is another example in which bill by account functionality can be used to track network traffic that may not be desirable to bill to an end point device owner or user, and bill by account functionality can be used to log and mediate such usage out of the user or end point device owner's bill.

[0532] Any end point device agent software required to connect to the intermediate networking device can also be implemented as a service processor 115 developer's kit as described herein and distributed to aid manufacturers, service provider and virtual service providers in bringing new devices onto networks with intermediate networking device capability.

[0533] In the case of a femto cell intermediate networking device, in some embodiments, it is desirable to facilitate handover from the WWAN network to the femto cell. In some embodiments, this provided in the intermediate networking device service processor 115 in a variety of ways. In some embodiments, the voice and data traffic is routed through a VPN tunnel controlled by the service processor 115 and connected to a network element, such as the transport gateway or another specified traffic concentration destination for the femto cell. In some embodiments, the voice traffic, the data traffic or both can be routed in secure or open Internet channels to different destinations, or the data can be routed directly to the Internet destination specified by the packets. In some embodiments, the femto cell intermediate networking device controls the femto cell frequencies or local frequency channel strength surveys over the intermediate networking device control channel. In some embodiments, the service processor 115 has a VPN connection to a network base station hand off controller to assist in handoff to and from the WWAN network and/or has the capability to instruct the end point device and the base station handoff controller. In some embodiment, whenever an end point device authenticated for femto cell access is within range of the femto cell, the service

provider desires to set up a service processor 115 profile to get the end point device to connect to the femto cell even if it has a strong signal with one or more WWAN base stations so that the WWAN traffic may be offloaded. In some embodiments, the service processor 115 can form a secure control plane link with network AAA functions to manage authorization and admission of end point devices the femto cell has not yet admitted, or the network policies can require re-authorization every time a end point device attempts access. Once an end point device is connected to the femto cell intermediate networking device, the verifiable traffic monitoring, control and billing functions described herein can be applied to various application embodiments. For example, the intermediate networking device service policy verification techniques disclosed herein, as similarly described with respect to various device embodiments, can similarly be applied to the femto cell intermediate networking device embodiments.

[0534] In some embodiments, the service provider desires to keep the number of end point devices or users that access an intermediate networking device below a certain count specified in the service processor 115 profile. In some embodiments, this is accomplished by controlling the number of IP addresses allowed onto the intermediate networking device local area side connection. In some embodiments, this is facilitated by observing the end point device identification parameters available in the end point device traffic. In some embodiments, this is facilitated by observing the traffic patterns to determine the likely number of devices connecting to the network. For example, traffic demand patterns can be examined to determine how many users are likely to be demanding access at one time. Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

INCORPORATION BY REFERENCE

[0535] This application incorporates by reference the following US applications:

[0536] Application No. 12/380,780 entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed March 2, 2009; provisional Application No. 61/206,354 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed January 28, 2009; provisional Application No. 61/206,944 entitled SERVICES POLICY COMMUNICATION

SYSTEM AND METHOD, filed February 4, 2009; provisional Application No. 61/207,393 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009; and provisional Application No. 61/207,739 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 13, 2009.

WHAT IS CLAIMED IS:

1. A system, comprising:
 - a processor of a communications device configured to:
 - store a first set of device credentials for activating the communications device for a first service on a first network; and
 - send an access request to the first network, the access request including the first set of device credentials; and
 - a memory of the communications device coupled to the processor and configured to provide the processor with instructions.

ABSTRACT OF THE DISCLOSURE

Various embodiments are disclosed for a services policy communication system and method. In some embodiments, a communications device stores a set of device credentials for activating the communications device for a service on a network; and sends an access request to the network, the access request including the set of device credentials.

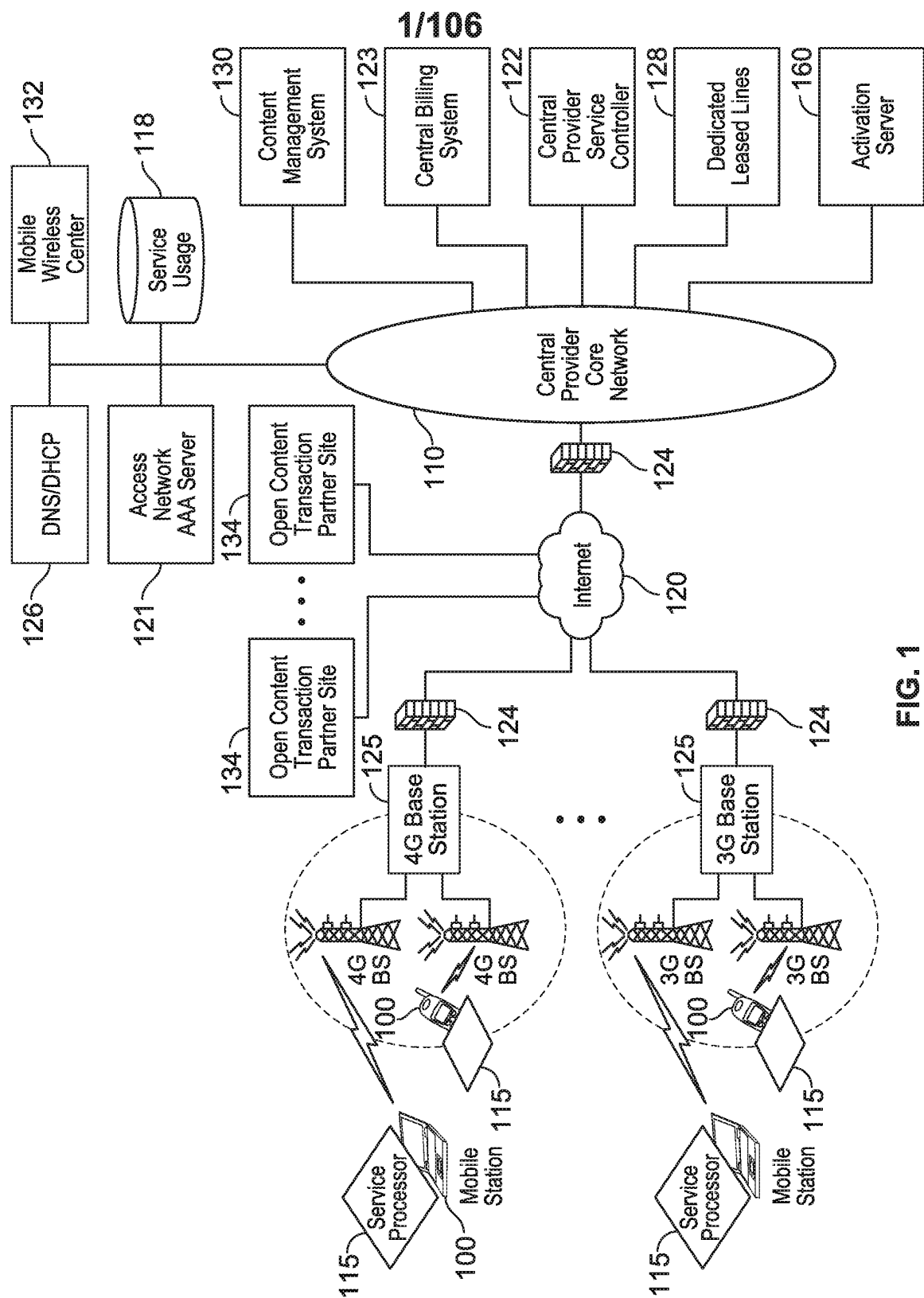


FIG. 1

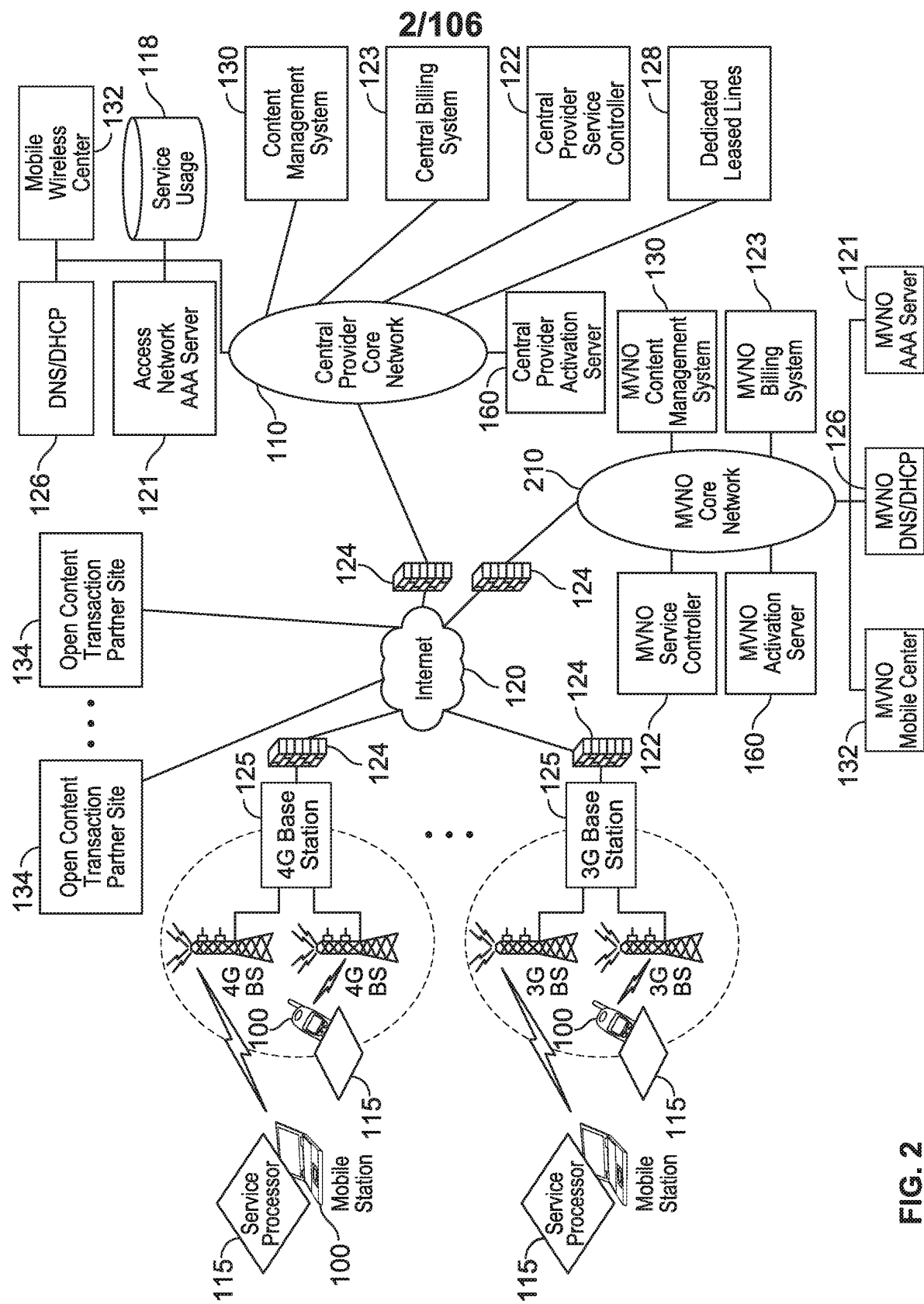
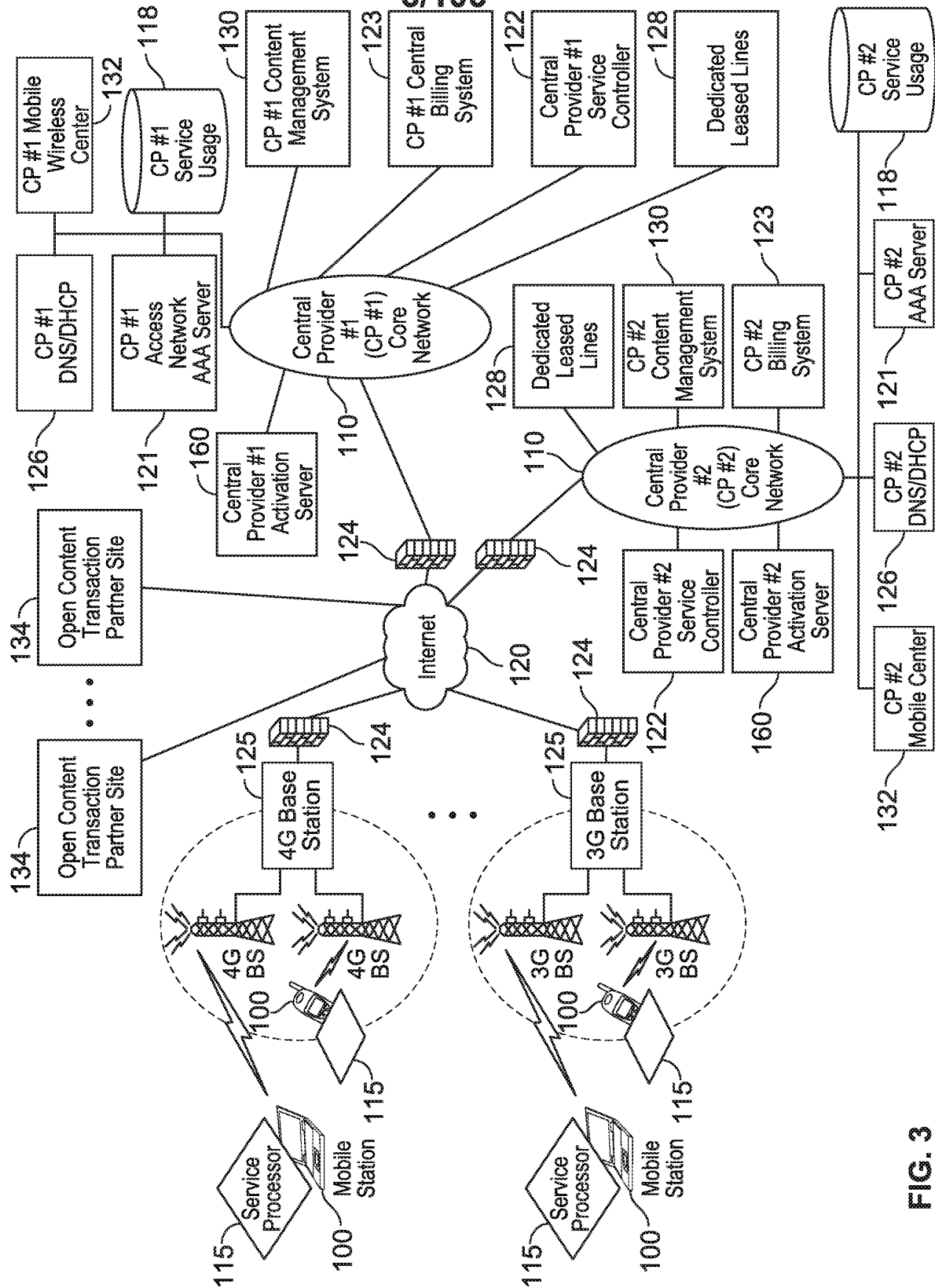


FIG. 2



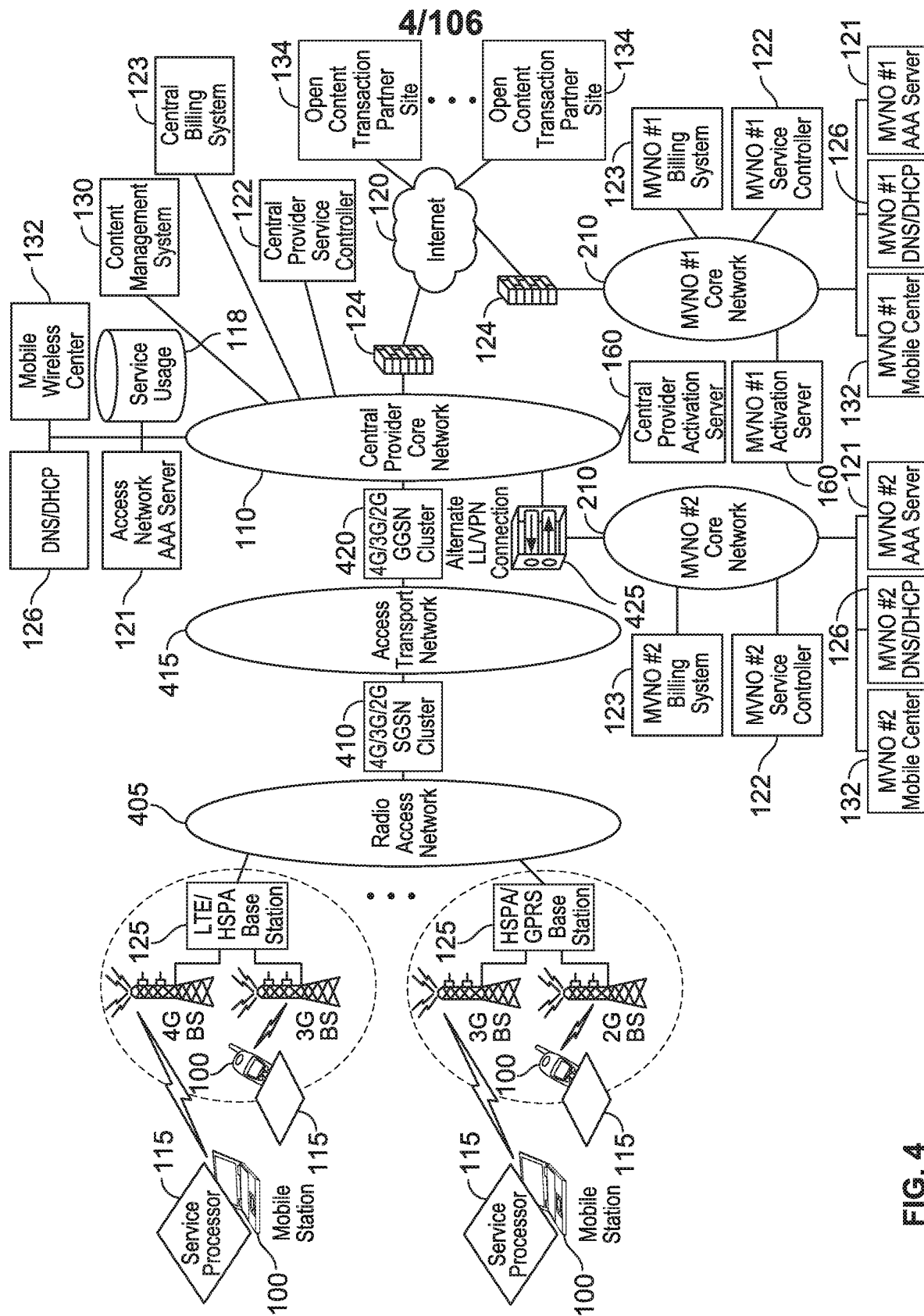


FIG. 4

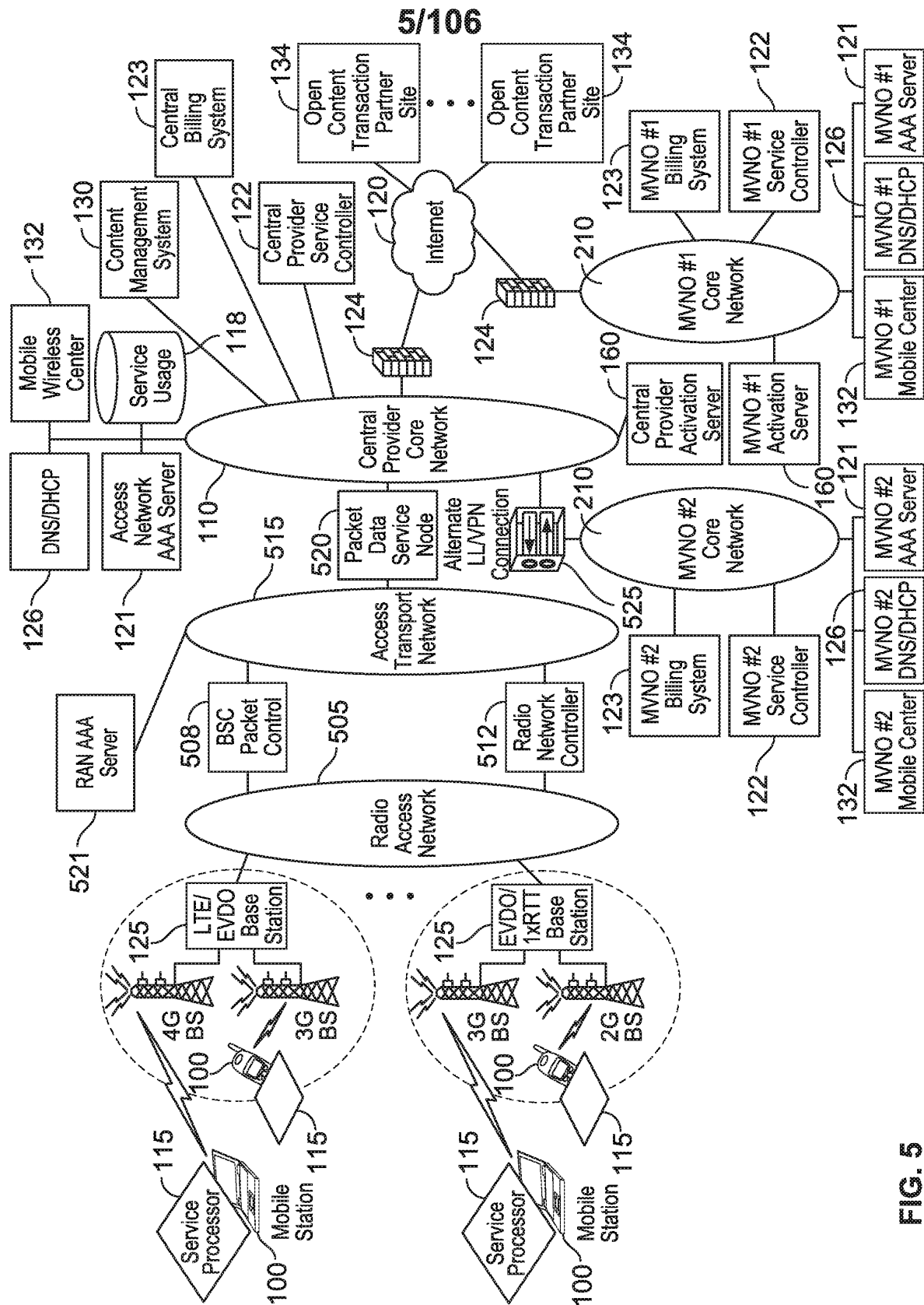


FIG. 5

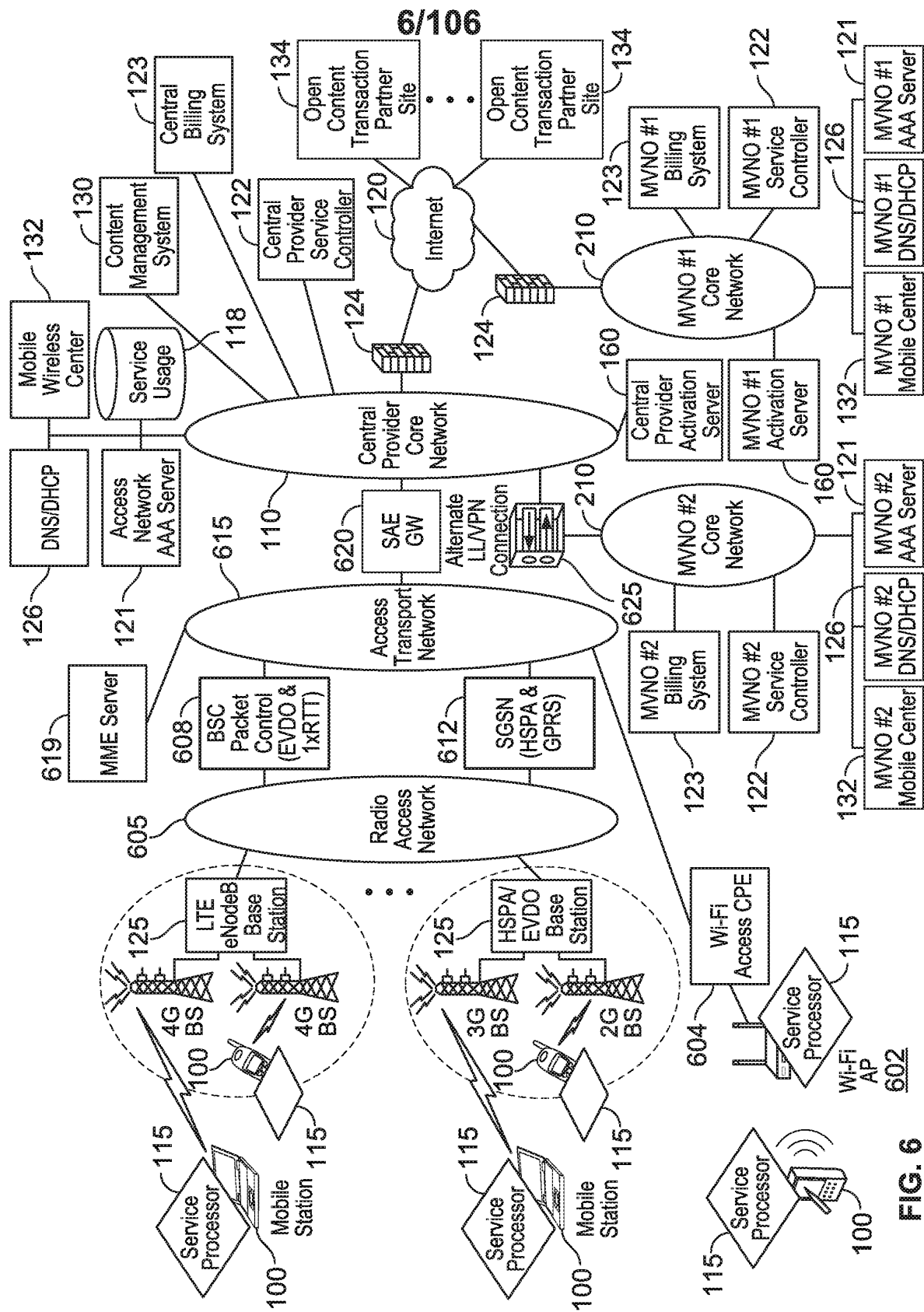
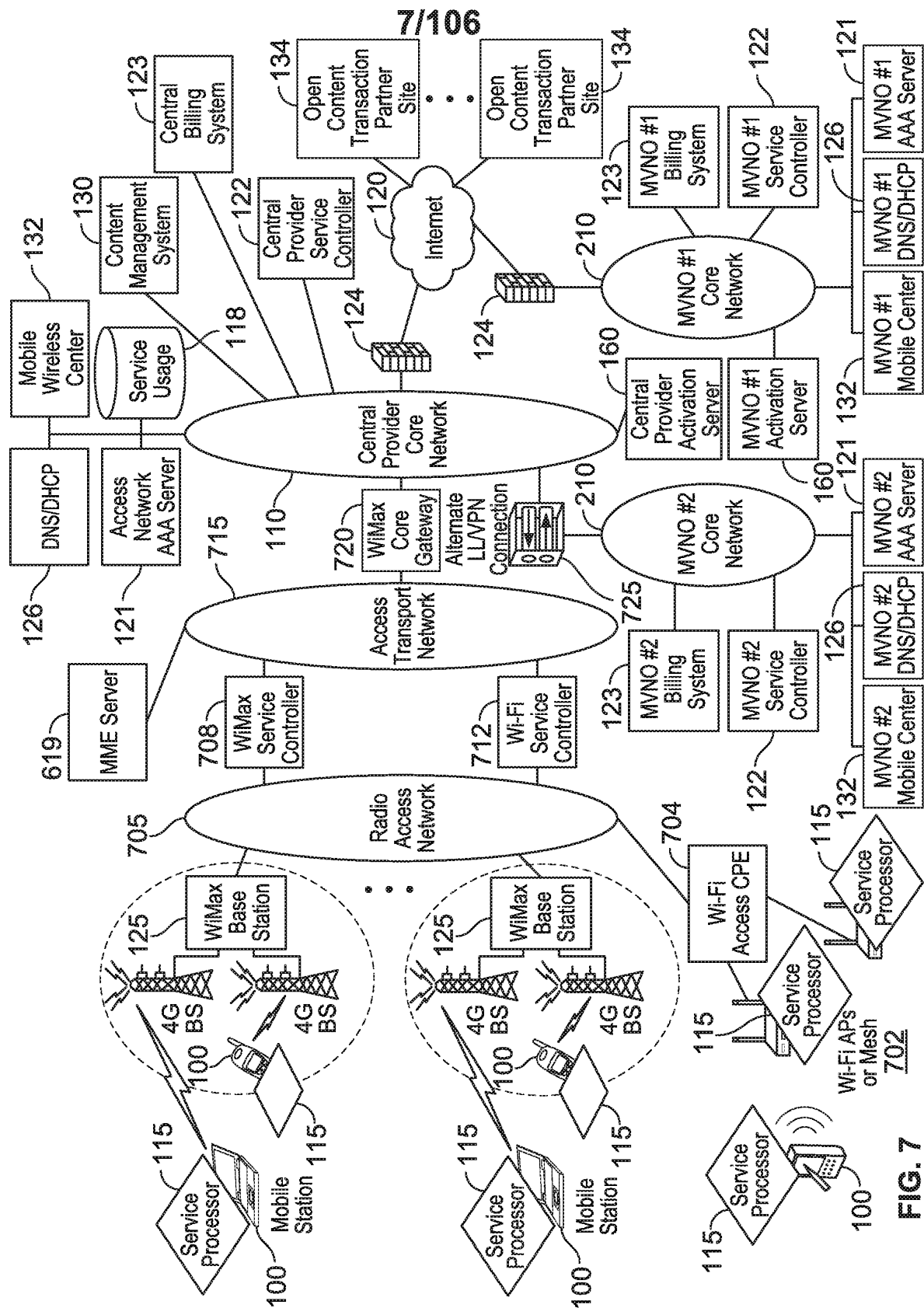


FIG. 6



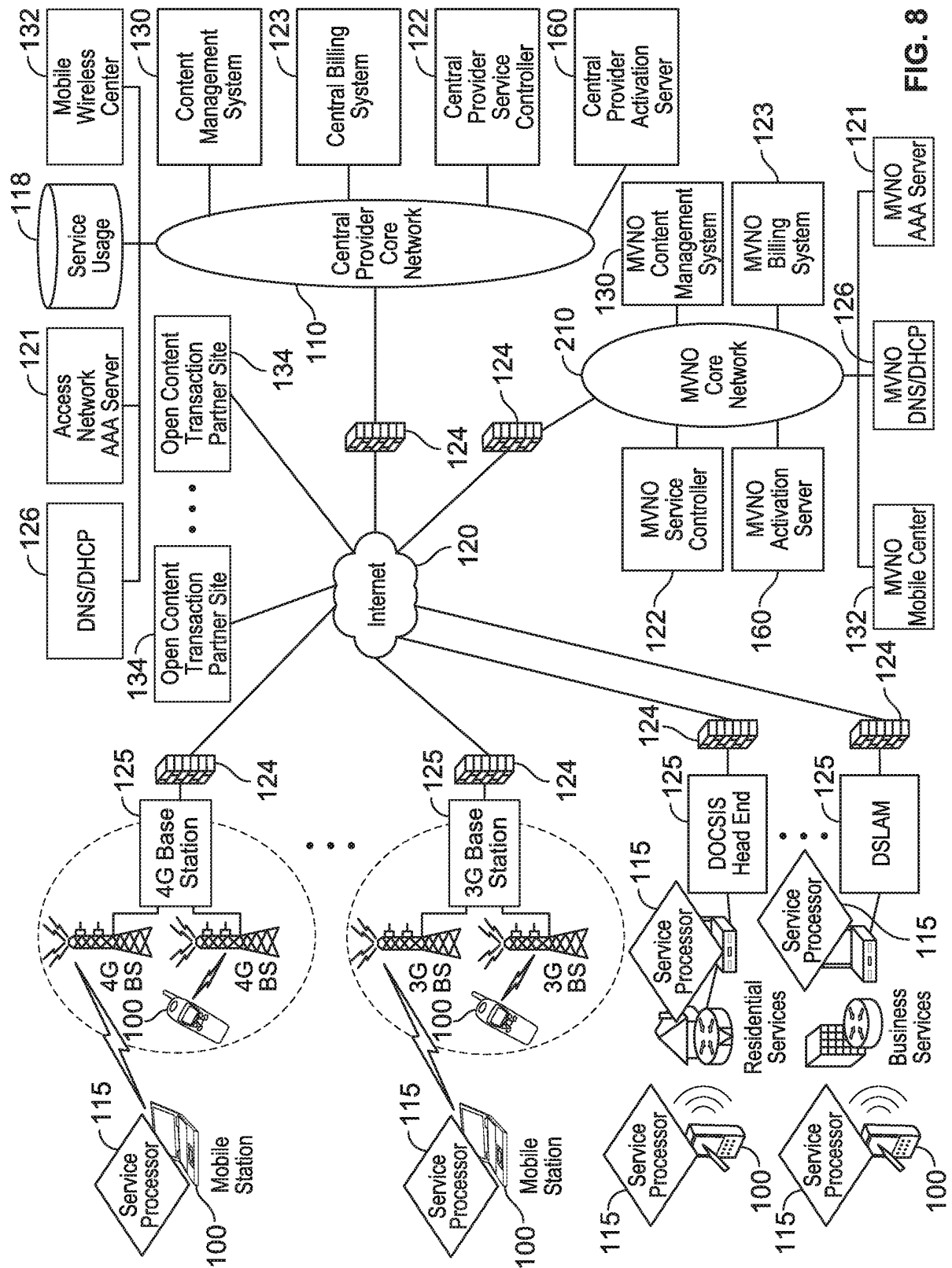


FIG. 8

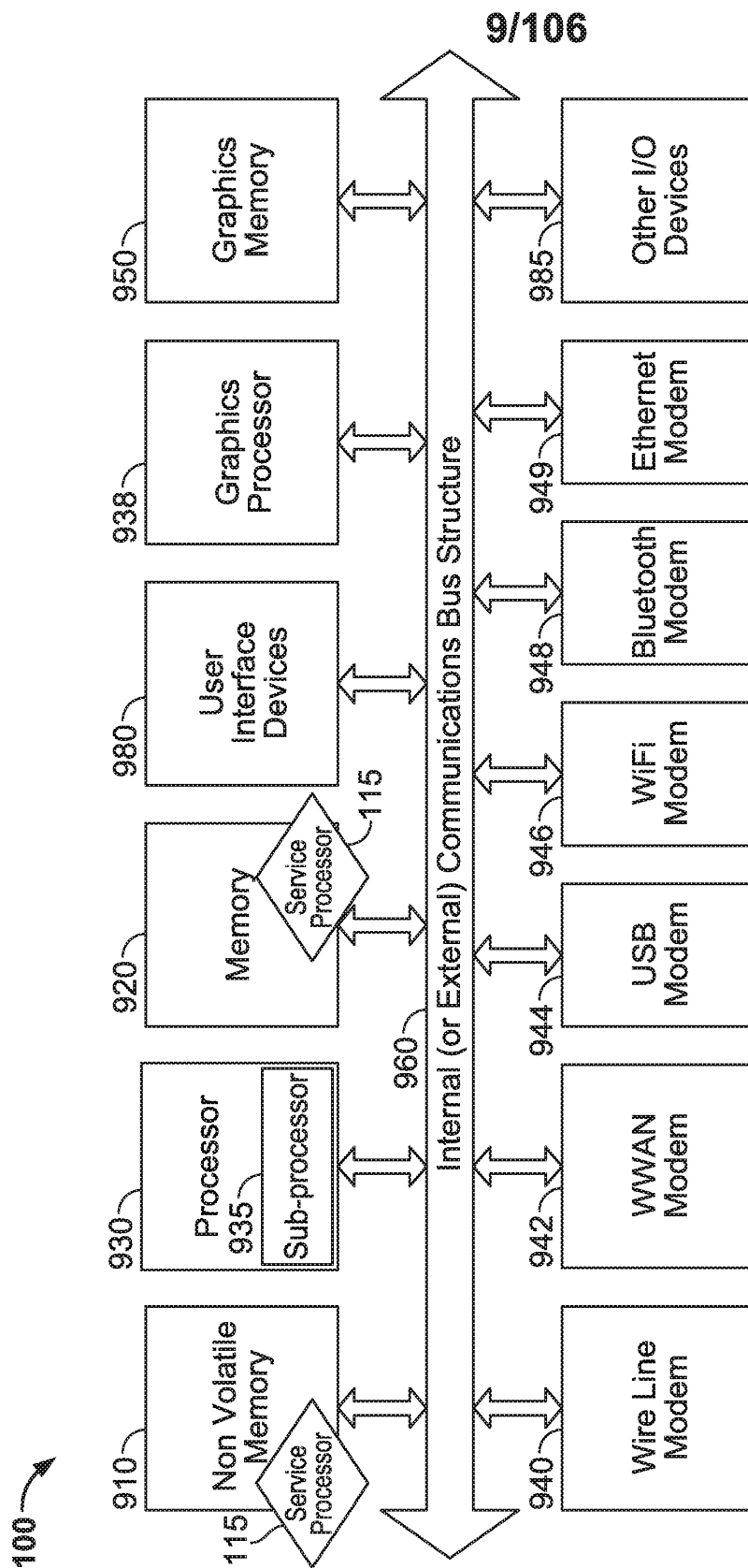


FIG. 9

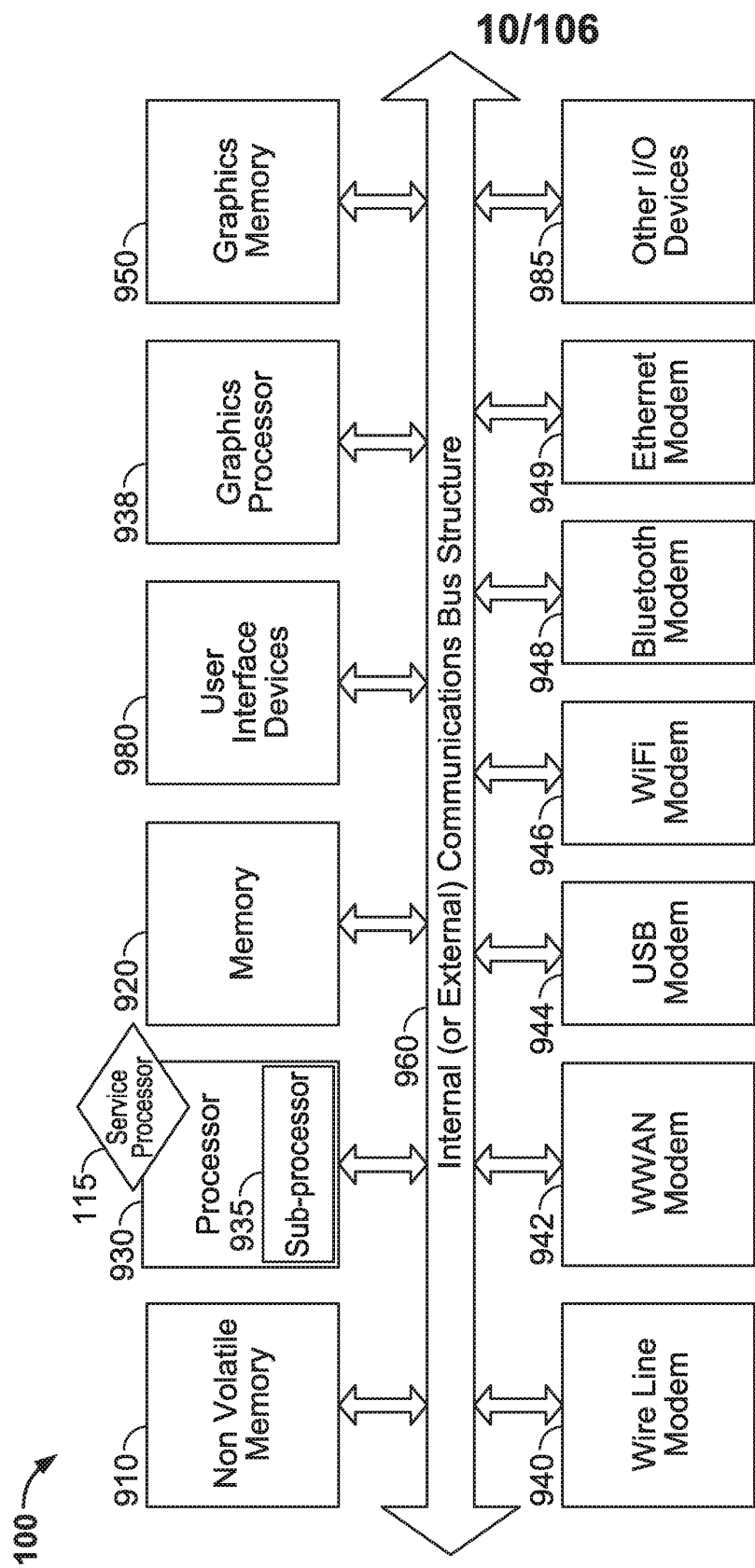


FIG. 10

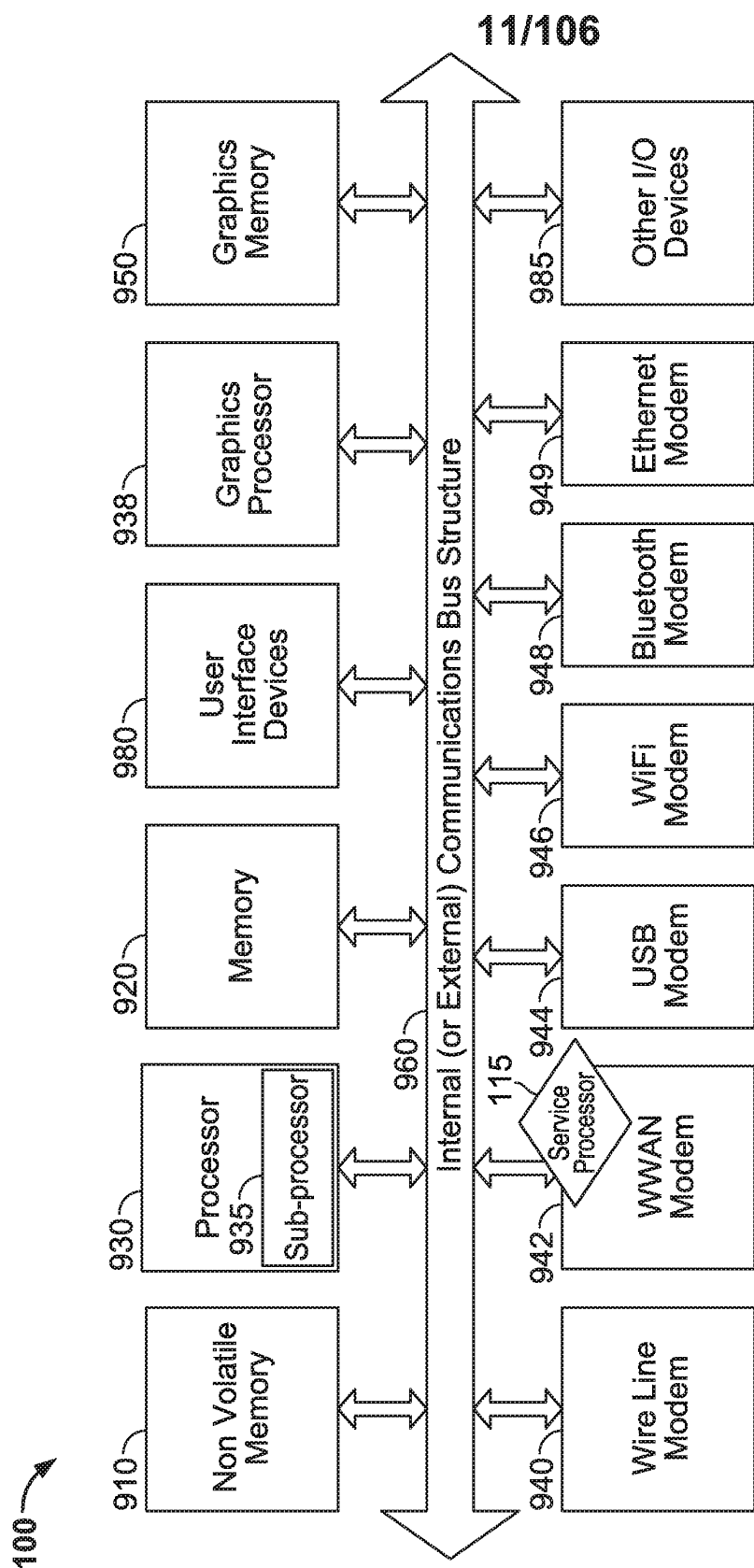


FIG. 11

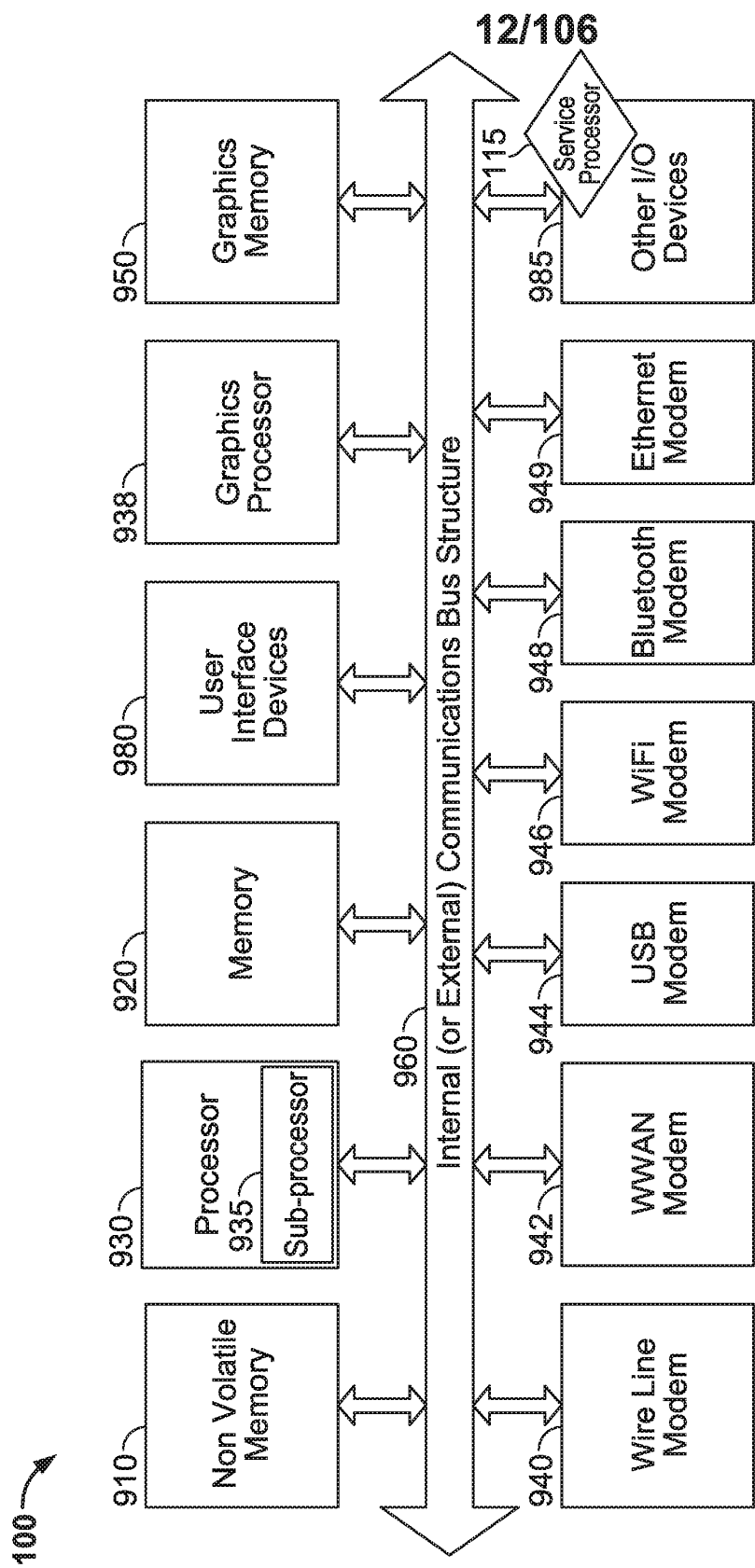


FIG. 12

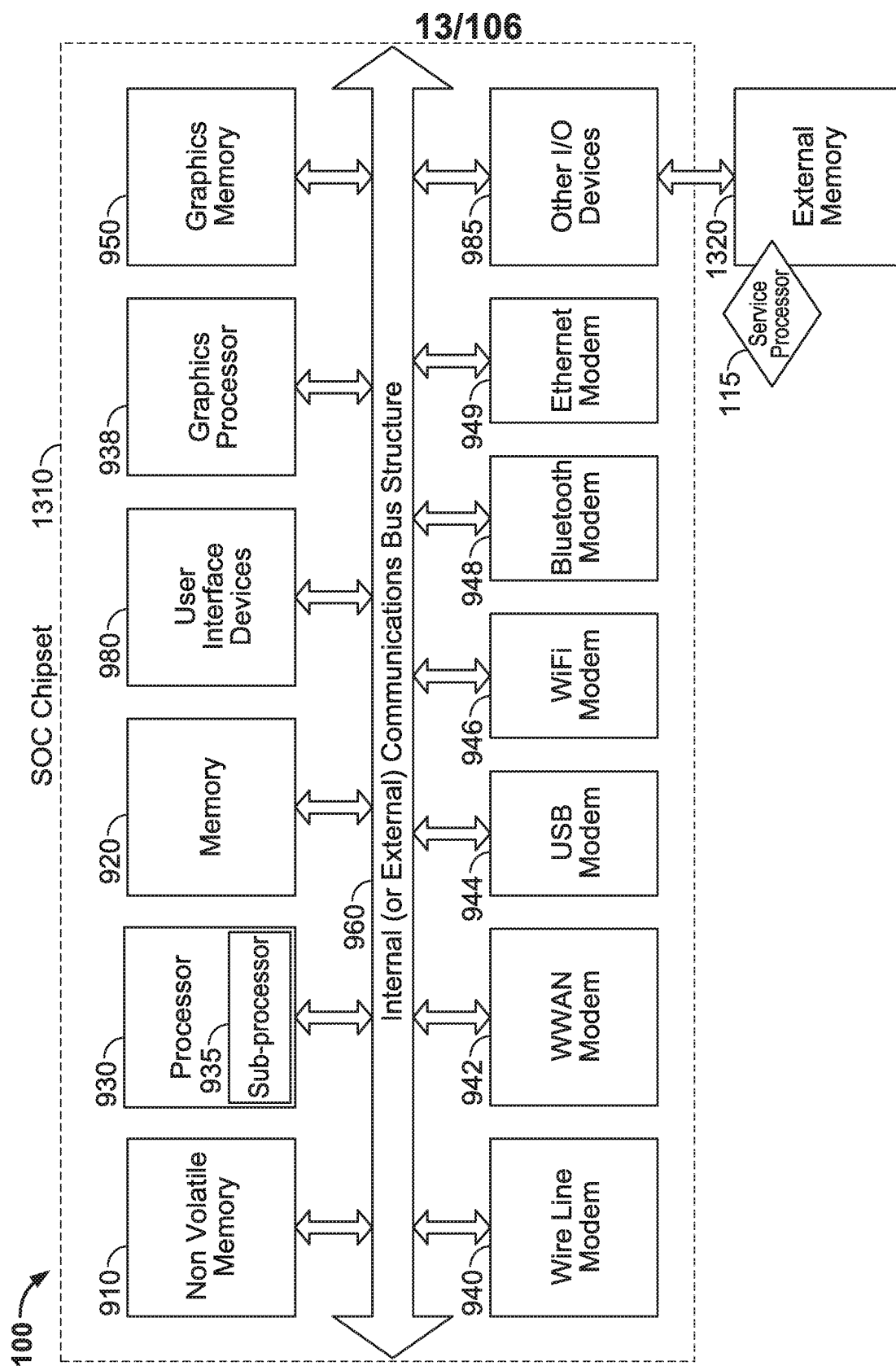


FIG. 13

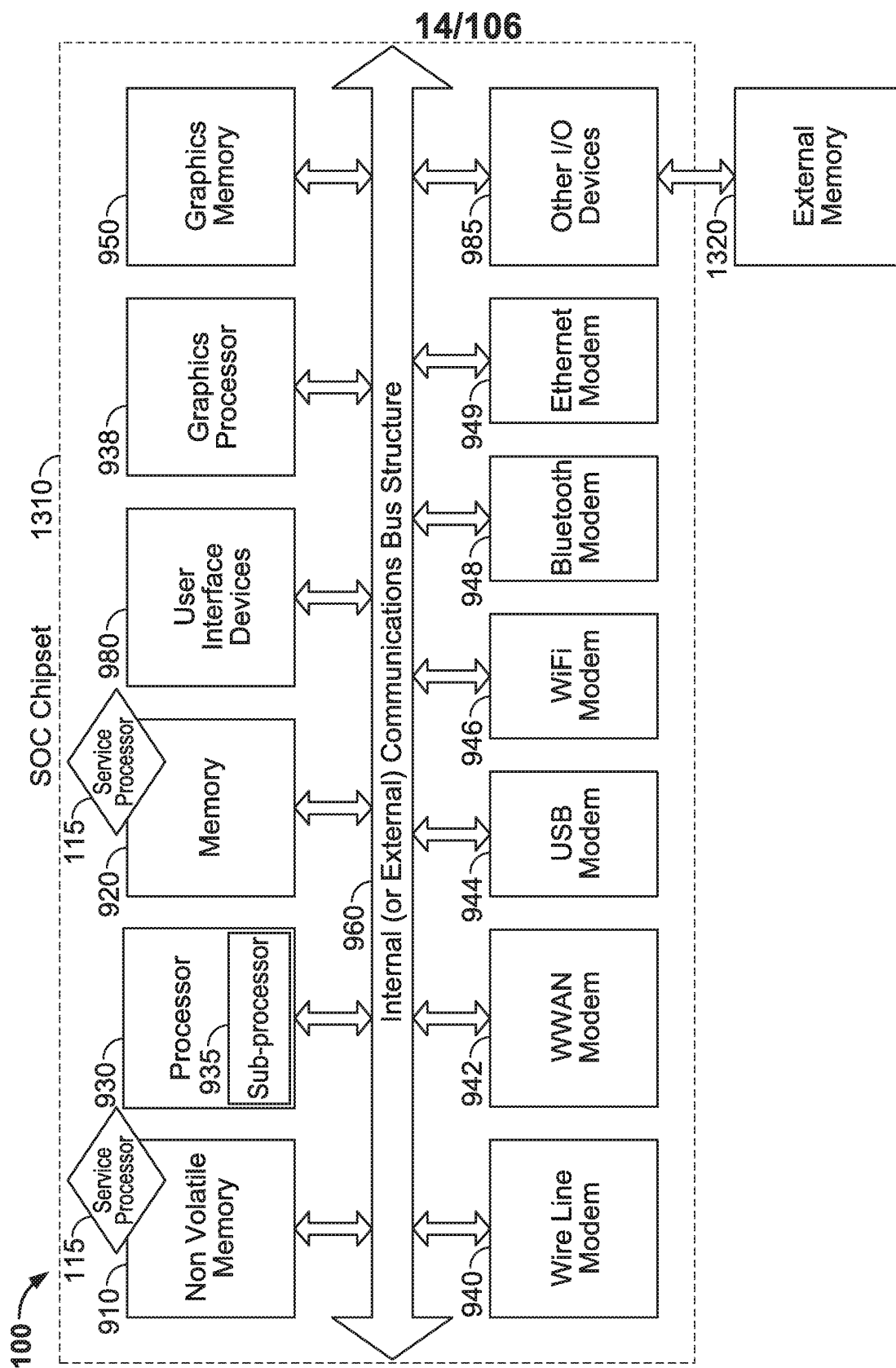


FIG. 14

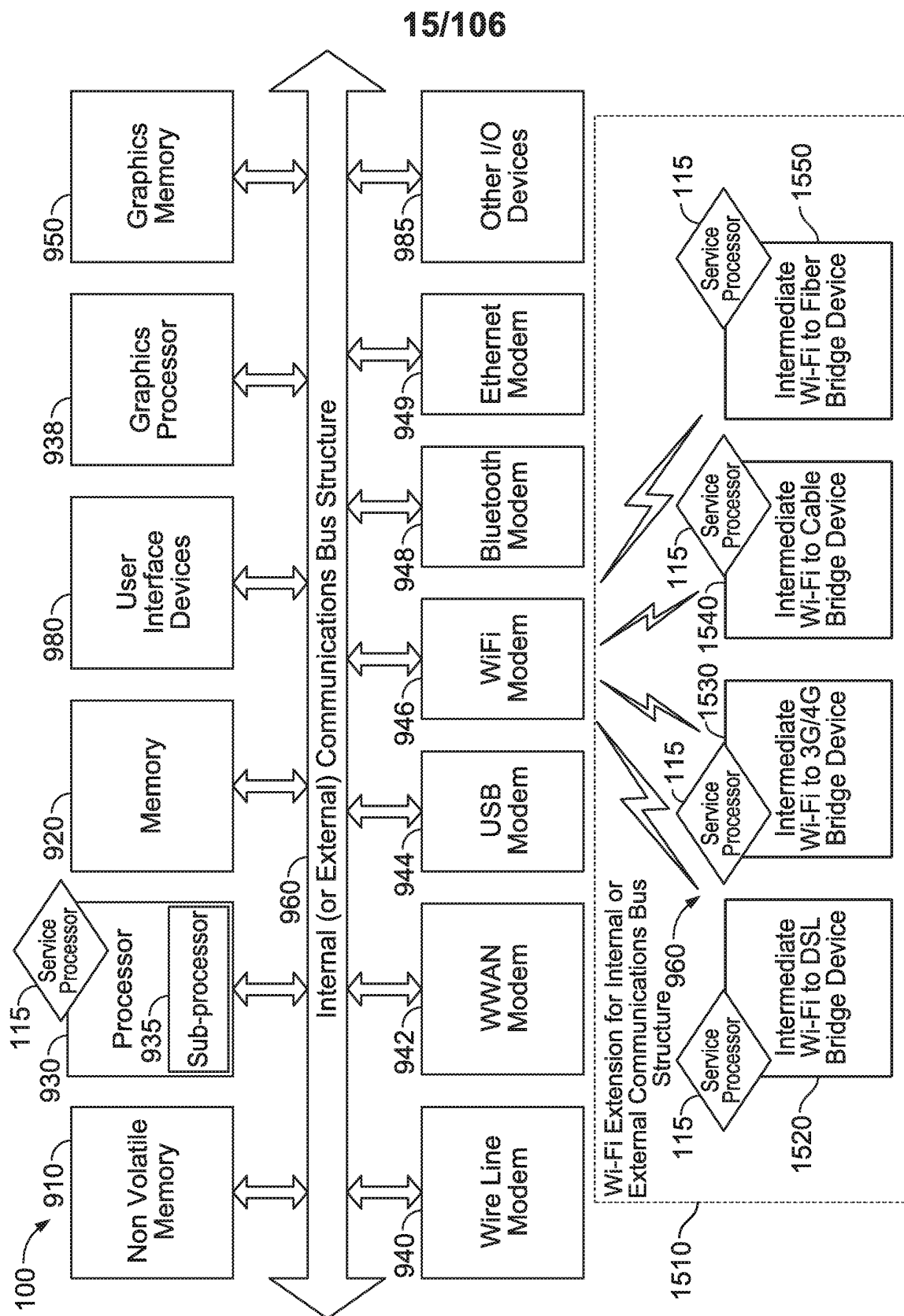


FIG. 15A

16/106

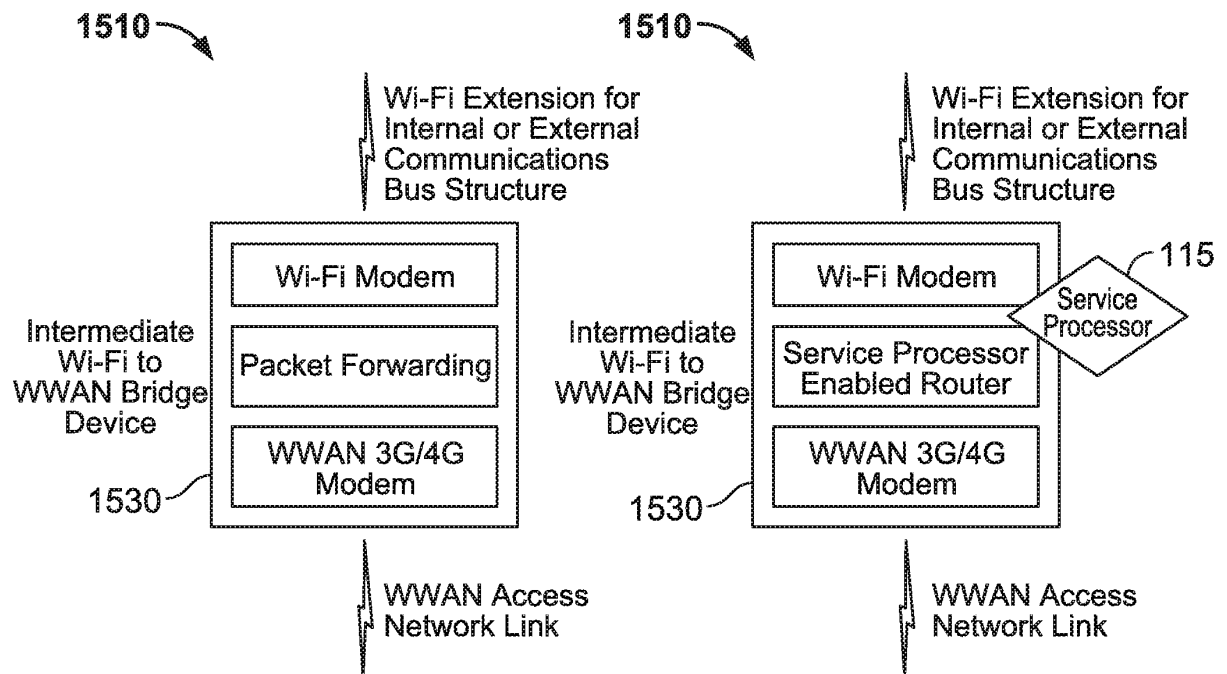


FIG. 15B

FIG. 15C

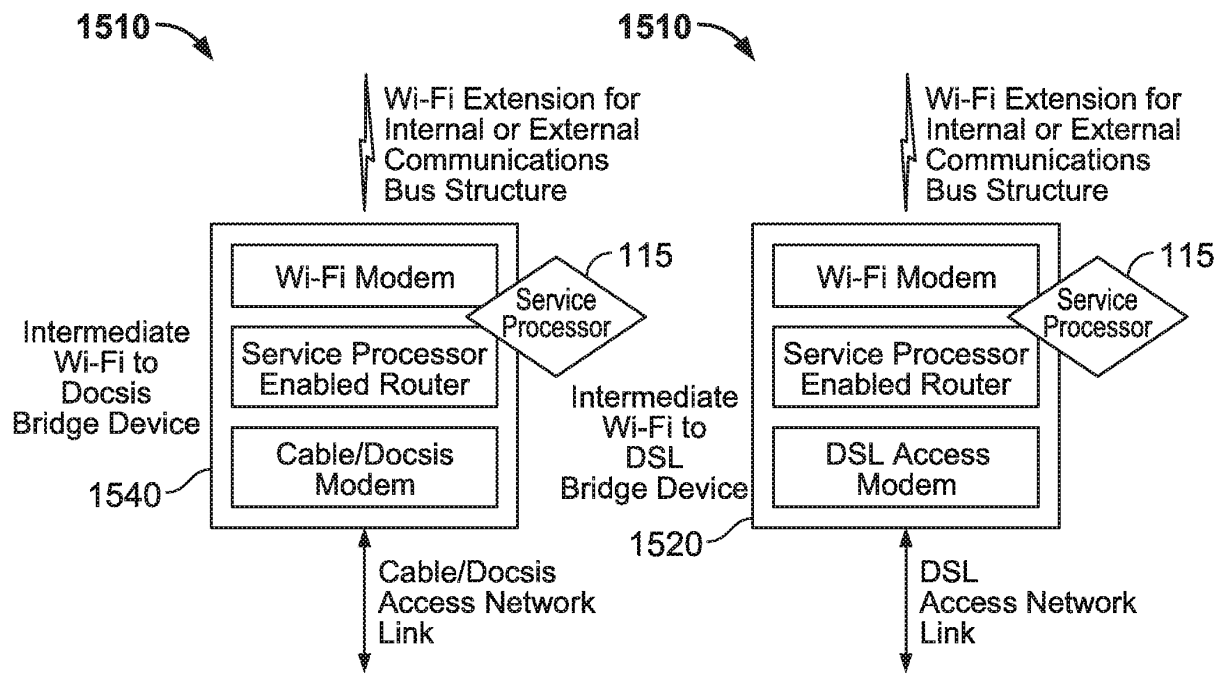


FIG. 15D

FIG. 15E

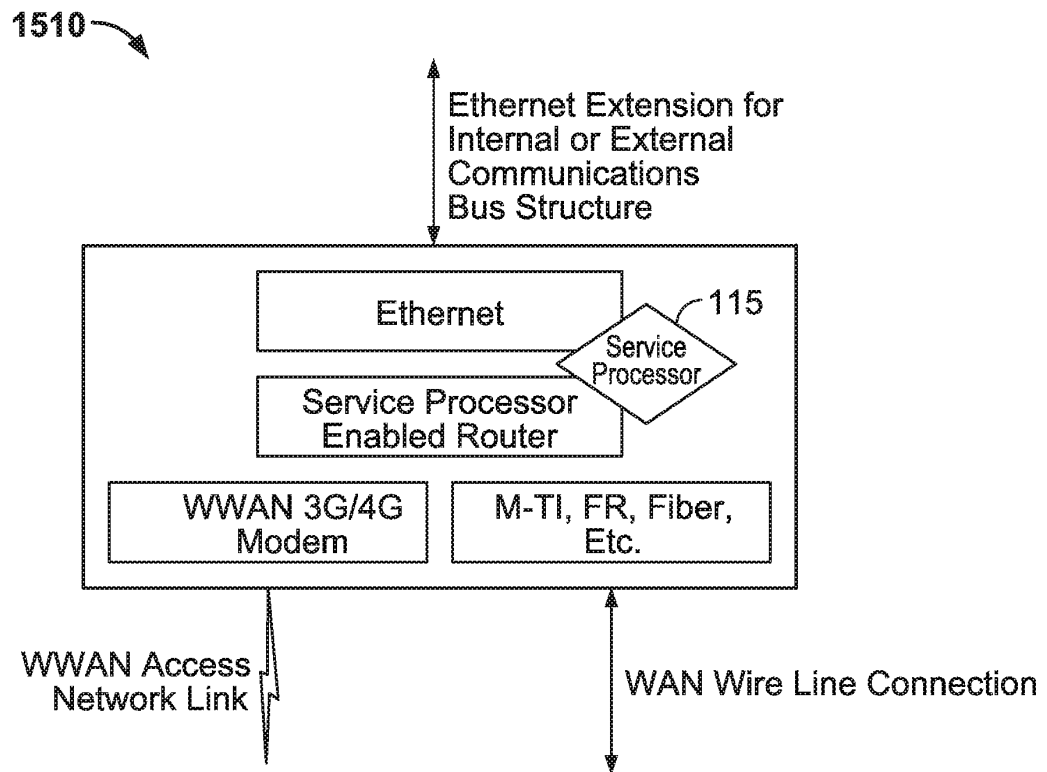


FIG. 15F

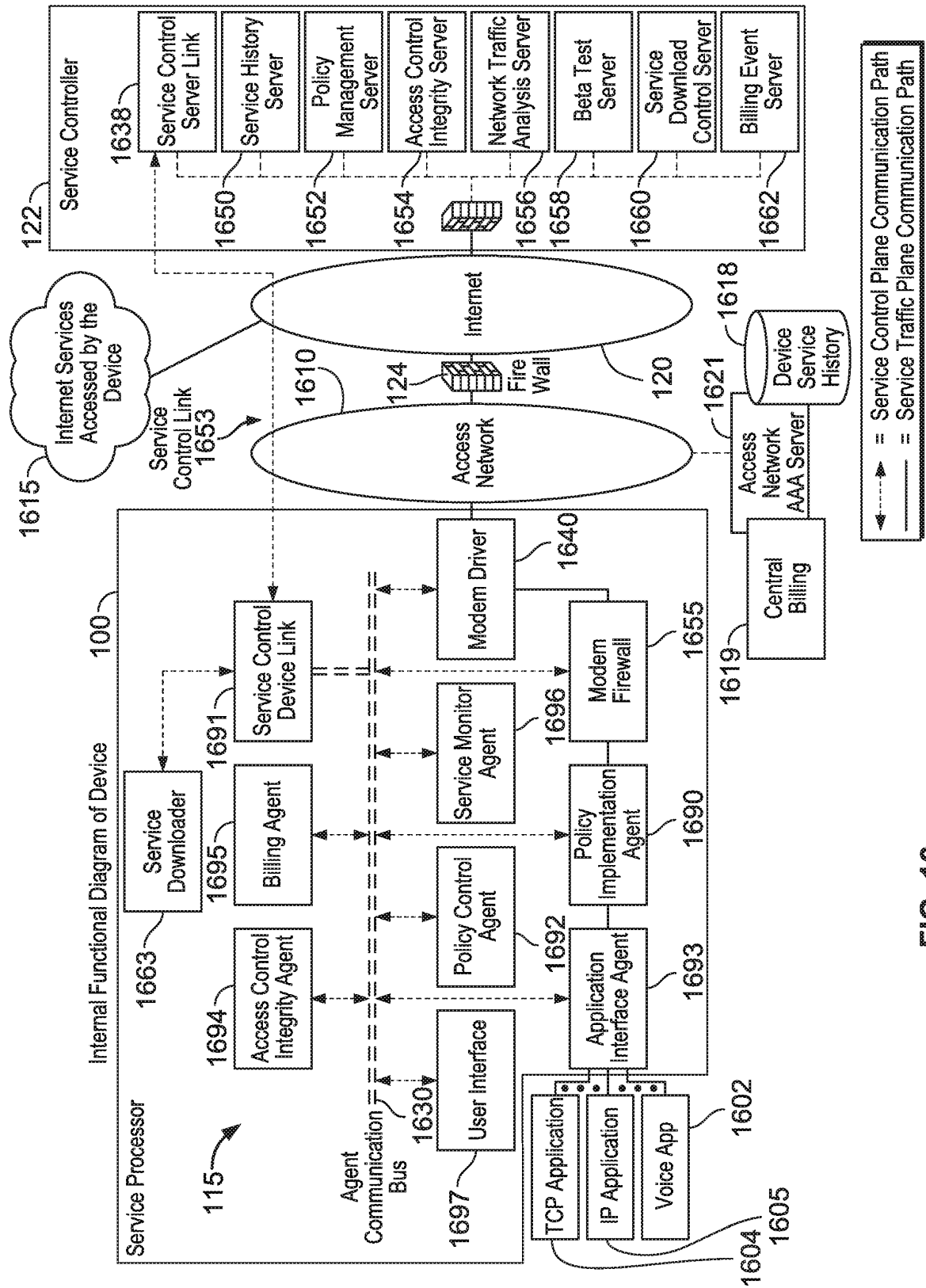
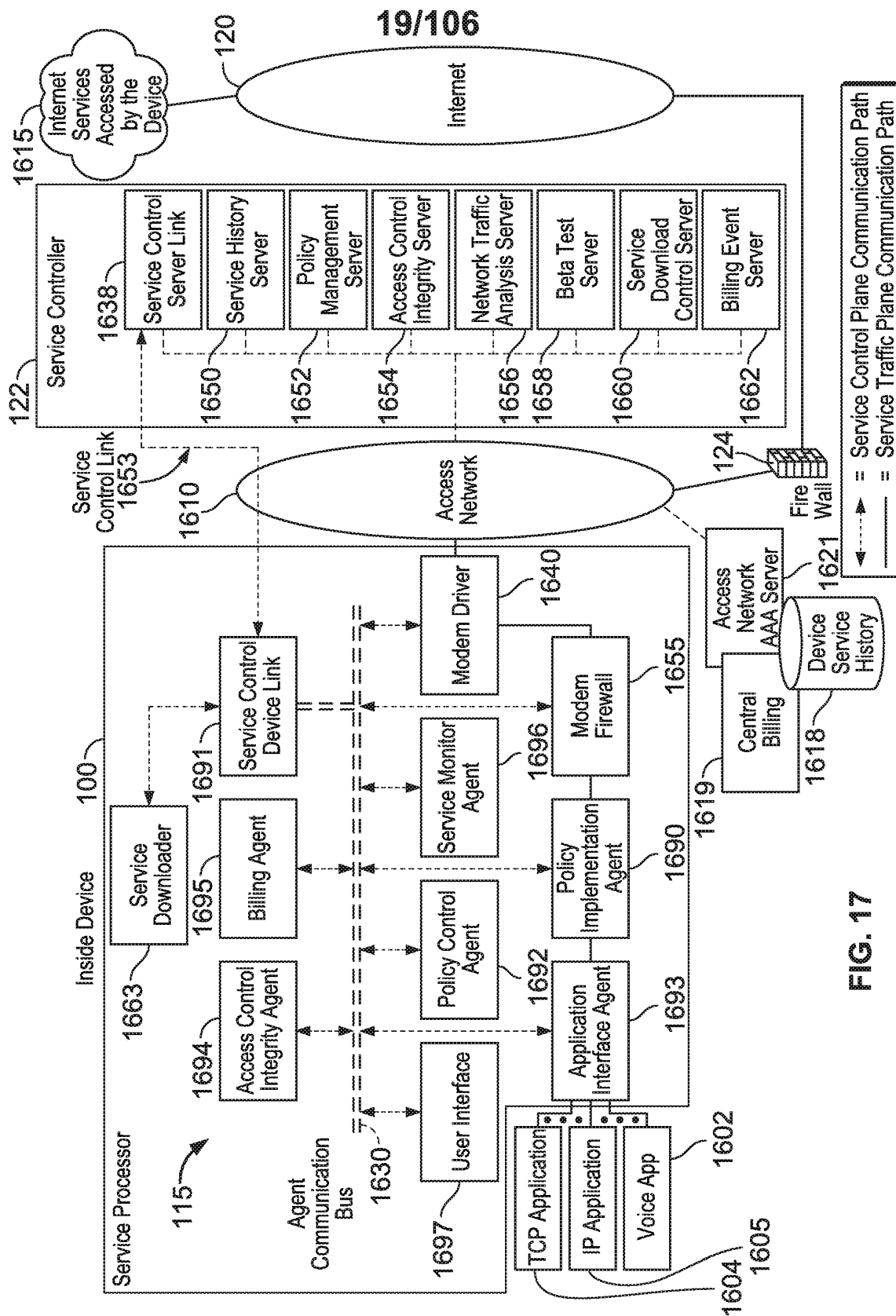
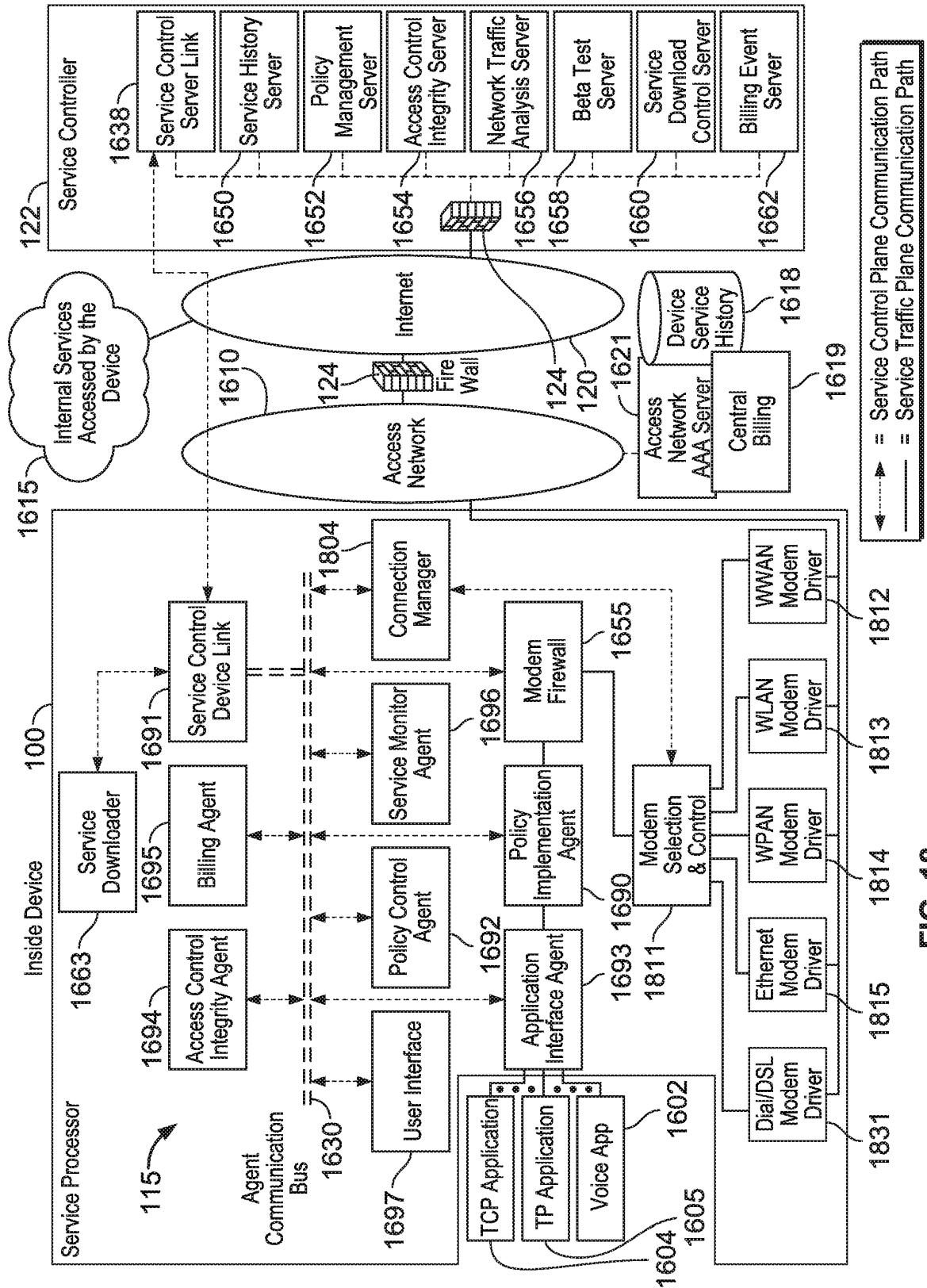


FIG. 16





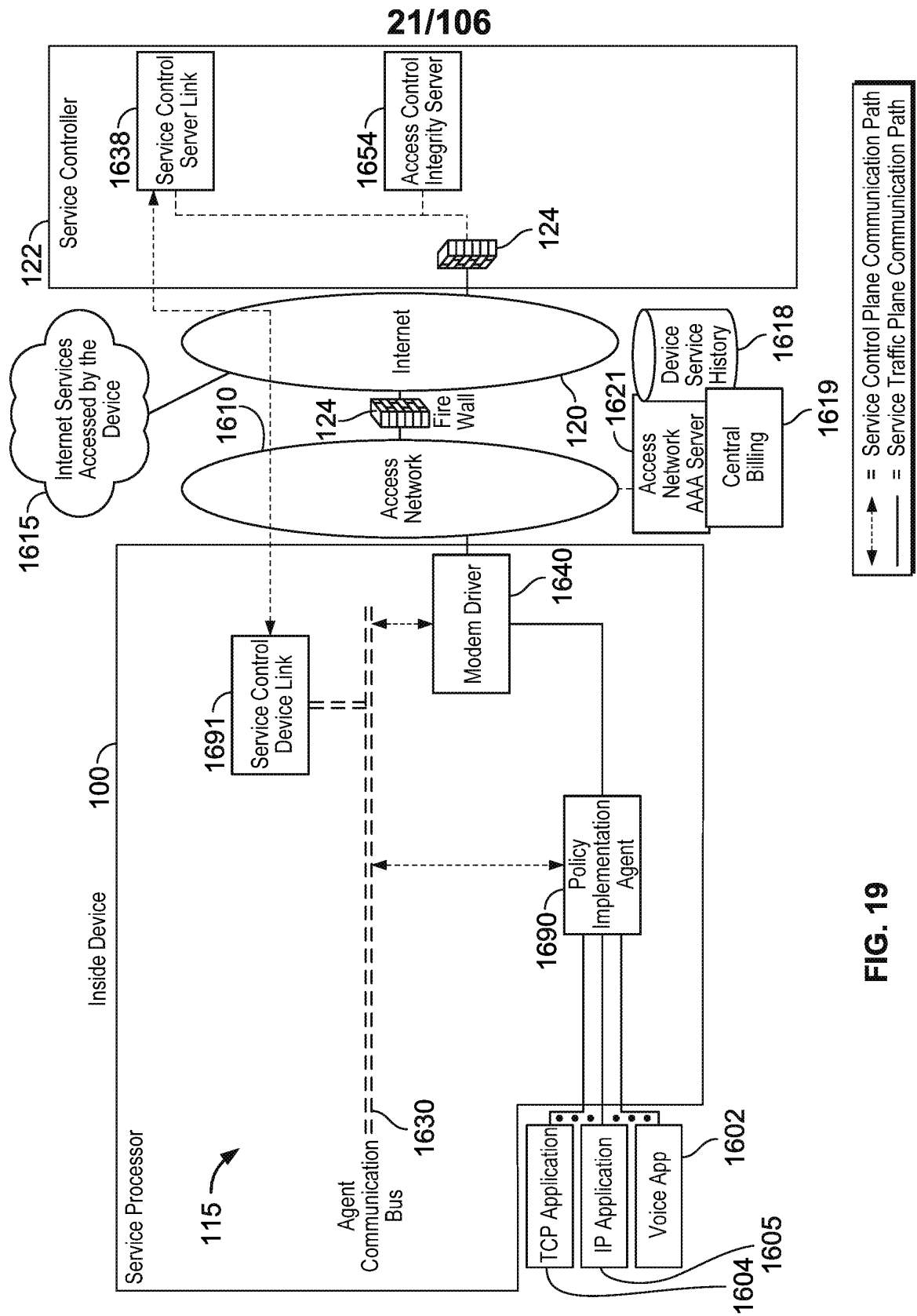


FIG. 19

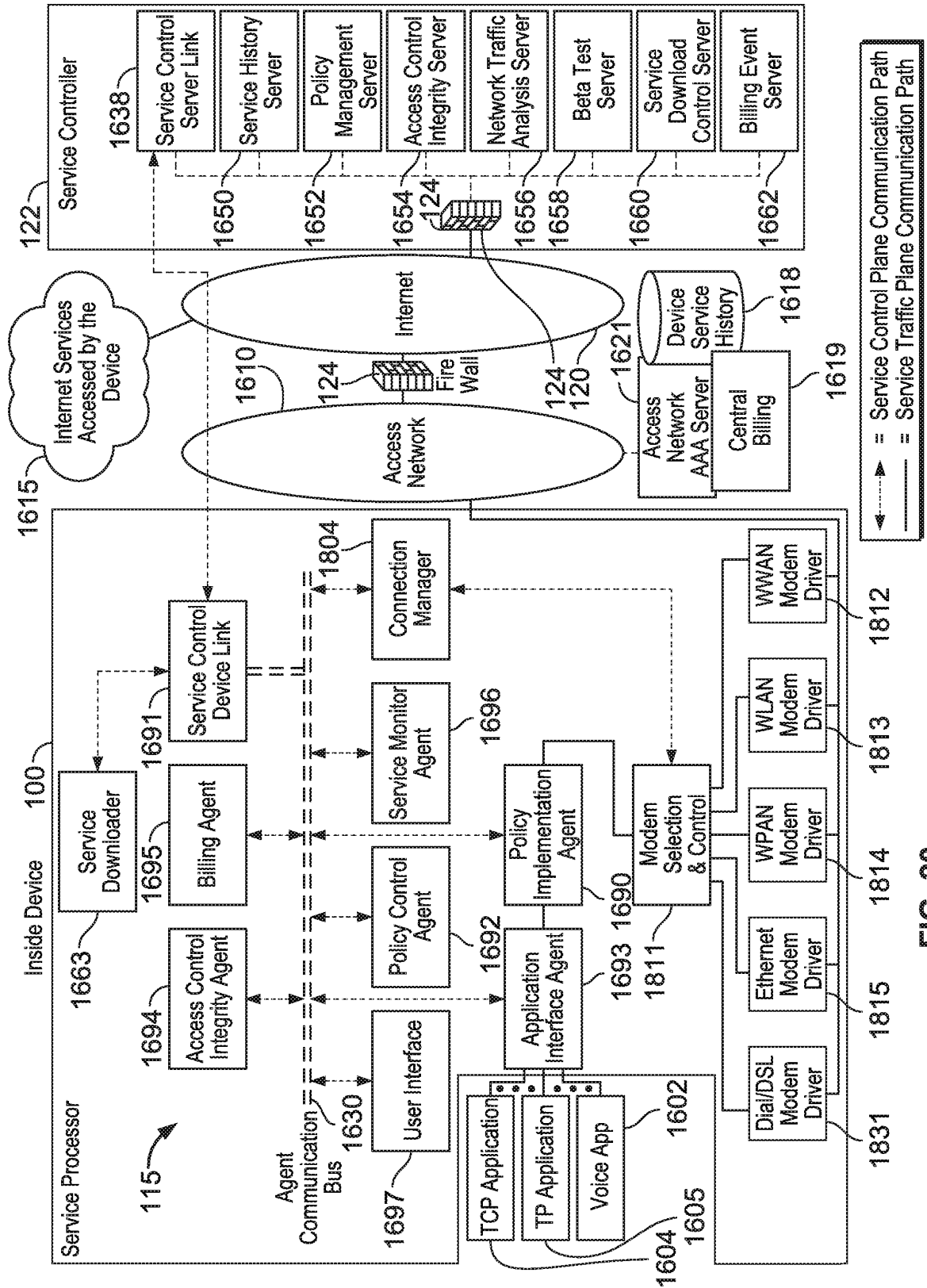


FIG. 20

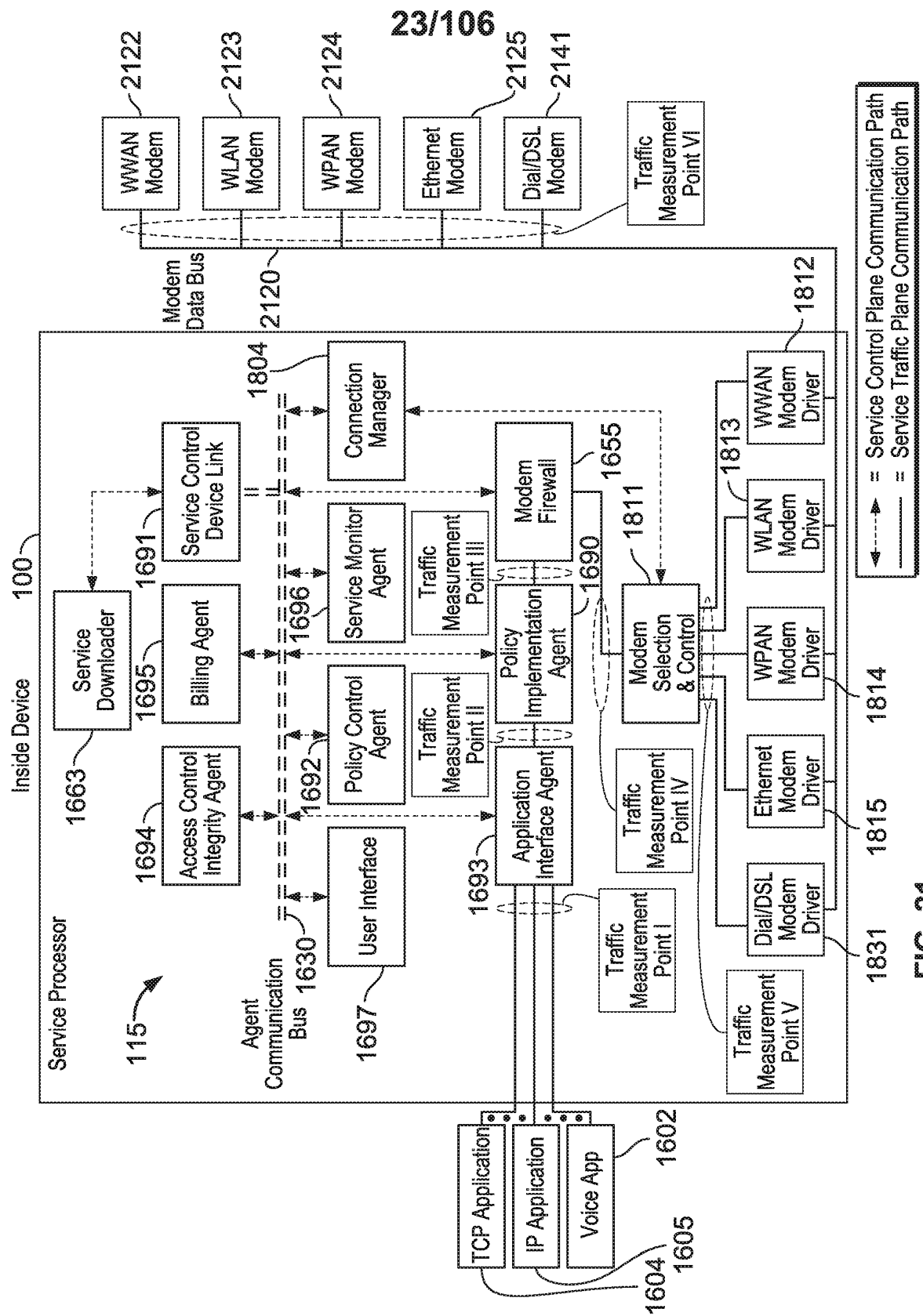


FIG. 21

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 115 to Service Controller. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Agent 1694	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, verifies configuration of other agents or performs challenge-response testing. In some embodiments, monitors software loading activity, protected memory access or communication with Service Processor agents to detect unauthorized changes to Service Processor software or configuration.
Policy Control Agent 1692	Takes policy instructions from the network and sets instantaneous device service policy. In some embodiments, performs a policy control function to adapt instantaneous service policies to achieve a service usage objective.
Policy Implementation Agent 1690	Implements traffic control and QOS policy rules for device. In some embodiments provides the functions of access control and/or firewall function or perform traffic inspection and characterization. In some embodiments packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed completely in the Policy Implementation Agent 1690.
Service Monitor Agent 1696	Records and reports device service usage. In some embodiments, assists in communicating application tagging of traffic flows through the networking stack policy implementation. In some embodiments, maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection.
Application Interface Agent 1693	Rich feature interface for device application programs. In some embodiments, identifies application level traffic, reports service usage or tags traffic for service QOS control. In some embodiments, interacts with applications or programs applications to arrange application settings such as email file transfer options or browser headers. In some embodiments, intercepts certain application traffic to modify traffic application layer parameters such as email file transfer options or browser headers. In some embodiments implements certain aspects of traffic control or other service policies. In some embodiments, provides the functions of traffic control, access control and/or firewall.
Modem Firewall 1655	Blocks or passes traffic based on service policies and traffic attributes. In some embodiments, assists in traffic flow tagging. In some embodiments provides the functions of traffic control and/or access control.
Billing Agent 1695	Detects and reports billing events. In some embodiments interacts with the User Interface Agent 1697 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.

FIG. 22A

User Interface Agent 1697	Provide service interface to users.
Service Downloader 1663	Provides a download function to install or update service software elements on the device.
Connection Manager 1804	Provides a control and supervision function for one or more modem drivers or modems that connect to an access network.
Modem Selection and Control 1811	Selects the access network connection.
Modem Drivers 1831, 1815, 1814, 1813, 1812	Converts data traffic into modem bus traffic for one or more modems.
Modems 2141, 2125, 2124, 2123, 2122	Connects the device to one or more networks.

FIG. 22B

Partial Summary of Embodiment Functions	
Service Controller 122 Element	
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 122 Service Processor 115 device agents. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Server 1654	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected.
Policy Management Server 1652	Transmits policies to the Service Processor 115.
Access Network AAA Server 1621	Provides access control and authorization functions for the device access layer. Records and reports device network service usage.
Service History Server 1650	Collects and records service usage reports from the Access Network AAA Server 121 and the Service Monitor Agent 1696. In some embodiments, maintains a history of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection. In some embodiments, this activity summary is further analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.
Central Provider Billing System 1619	Provides mediation function for central provider billing events. Accepts service plan changes. In some embodiments, provides updates on device service usage, service plan limits or service policies.
Billing Event Server 1662	In some embodiments, collects billing events, provides service plan information to the Service Processor 115, provides service usage updates to the Service Processor 115, serves as interface between device and central Provider Billing System 123, or provides trusted third party function for certain ecommerce billing transactions.
Network Traffic Analysis Server 1656	Collects service usage history for devices or groups of devices and analyses the service usage. In some embodiments, presents service usage statistics in various formats to identify improvements in network service quality or service profitability. In other embodiments, estimates the service quality or service usage for the network under variable settings on potential service policy. In other embodiments, identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.
Beta Test Server 1658	Publishes candidate service plan policy setting to one or more devices. In some embodiments, provides summary reports of network service usage or user feedback information for one or more candidate service plan policy setting. In some embodiments, provides a means to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further setting optimization.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.
Transaction Server 134	Provides an electronic commerce offering and transaction platform to the device.

FIG. 23

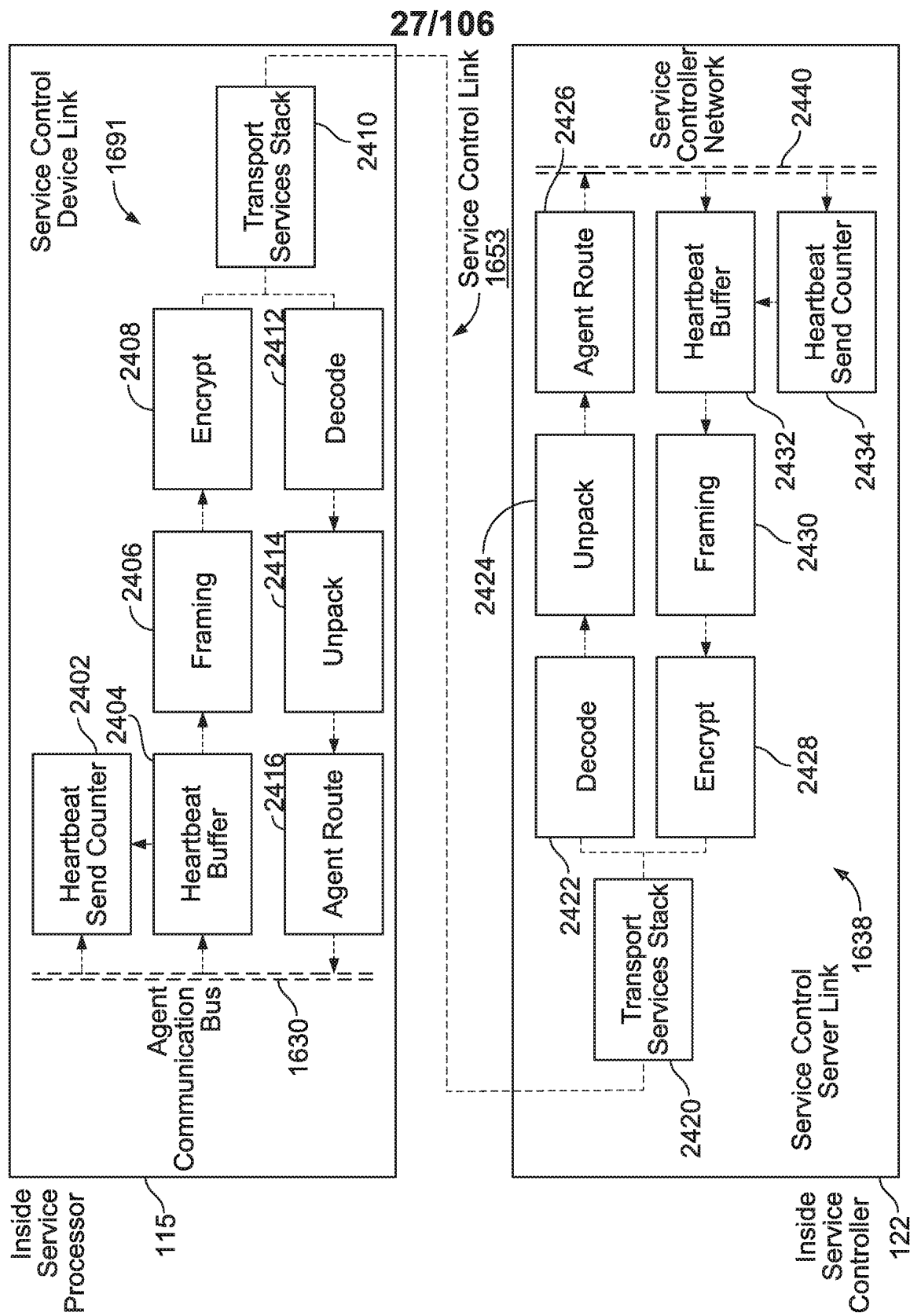
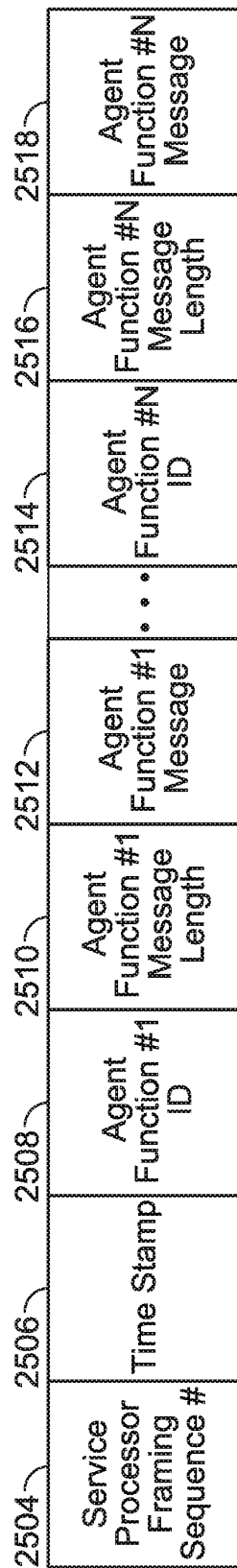
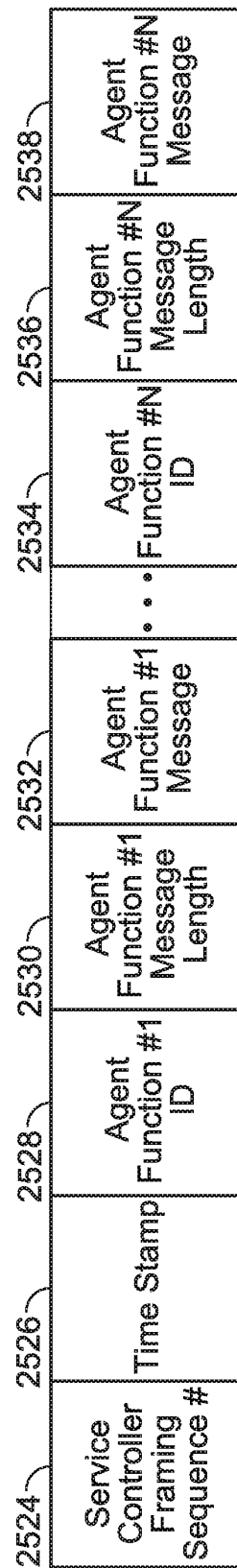


FIG. 24



Service Processor Communication Frame 2502

28/106



Service Controller Communication Frame 2522

FIG. 25

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Access control integrity report	Contains the latest results of the Access Control Integrity agents Service Processor system checks and reports any error events.	Not necessary to report in every heartbeat if there are no errors. Can report only on error, set a minimum frequency or respond to Service Controller polling.
Service monitor report	Reports filtered summary of Service Monitor Agent measurements. Summary reduces control traffic and filters out unauthorized private information.	Every heartbeat. Some embodiments link this to amount of data usage in the data path to keep overhead low. Report immediately upon polling from Service Controller.
Billing event report	Reports any billing activity since the last heartbeat. Billing events may include service usage events, transaction events, bill by account records, bill by account offset reports or any other event that results in a billing event report.	Send upon billing event. Report immediately upon polling from Service Controller.
Service Processor settings report	Reports service policy settings for all Service Processor agents.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Customer resource management report	Reports filtered summary of Service Monitor Agent measurements or filtered summary of other device or user activity such as service preferences, advertisement behavior and location. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Responses to Service Processor agent queries	Sends agent responses to challenge-response queries from the Service Controller.	Report immediately upon polling from Service Controller.

FIG. 26A

Location tracking service update	Reports filtered summary of location tracking information. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments call for a minimum time based transmission frequency.
Service usage based transmission frequency	Lowers overhead by buffering and reserving heartbeat communications from agents and servers until a certain amount of data has been transmitted or received in the network, or a certain amount of service has been consumed. When the parameters are chosen properly, this can result in the network control plane traffic overhead being a small percentage of data path traffic or result in the control plane traffic cost being a small percentage of the service usage cost.	Ranges depending on settings. For example, if there are 5 agents messages that typically need to be communicated, and each message is less than 100 bytes, and Service Processor heartbeat framing plus network overhead would result in a packet size of less than 1,000 bytes, and the heartbeat packet is transmitted when 10,000,000 bytes have been communicated over the data path, then the overhead loss due to one heartbeat packet in each direction is less than 0.02%.
Constant frequency transmissions	Since the device may be off line for long periods of time where the Service Control Processor needs to verify service control integrity, in some embodiments it can be advantageous to transmit heartbeat packets at a minimum rate regardless of data traffic activity. This is accomplished by setting a timer that sends queued heartbeat packets on a regular schedule.	Ranges depending on settings and applications.
Service Controller polled transmissions	In some embodiments, the Service Controller may poll the Service Processor for a heartbeat transmission at which time the Service Processor will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Controller.
Service Processor polled transmissions	In some embodiments, the Service Processor polls the Service Controller for a heartbeat transmission at which time the Service Controller will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Processor.

FIG. 26B

Agent self-check reports	Agent reports results of various agent self-diagnosis procedures to ensure that the agent is properly configured, operating properly, properly implementing service control policy or has not been tampered with. [provide examples which are extensions of typical software security self diagnosis reporting]	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Environment reports	One or more agents scan the storage or execution environment for one or more of the agents to identify potential threats to the integrity of the service implementation or agent integrity and makes a report. In one example embodiment, a scan is done to determine if unauthorized software or hardware is executing in a secure agent environment. In another embodiment, a scan is done to determine the software that has been loaded into a portion of the device operating environment, memory or storage, and the software list is referenced against a known threat list. In another example embodiment, the list of entities that accessed one or more agents is scanned to determine if an unauthorized access to an agent has occurred. In another embodiment a scan is performed to determine if unauthorized access to secure execution environment, memory or storage has occurred. In another example embodiment, the network access pattern for the device is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity. In another example embodiment, the internal device software, memory or peripheral access pattern is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.

FIG. 26C

User notification response reports	Billing agent, UI agent or another agent logs user notification events and the response of the user to the notification event. In some embodiments these events may be cross-referenced to the notification policy that should be in force on the device and the device service usage to ensure that the proper notification sequences are being adhered to. In other embodiments, the user notification responses are logged and used to document user choices to notification events, billing event decisions, service control decisions or service cost control decisions. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly. In some embodiments, the user may be asked to acknowledge a service overage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service overage acknowledgement.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a user notification sequence action with the user. In some embodiments, the report is generated when there is a verification error of some kind that is identified.
User warning response reports	Billing agent, UI agent or another agent logs user warning events and the response of the user to warning event. In some embodiments the user response is used to determine if the user is in positive control of the device. In some embodiments the response is used to confirm that the user acknowledges a billing overage or other service cost event. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a warning sequence action with the user. In some embodiments the report is generated when there is a verification error of some kind that is identified.

FIG. 26D

Agent communication log reports	Reports entities that established or attempted to establish communication with the agents. In one embodiment, reports a list of entities and the number of times the entity communicated or attempted to communicate with the agent. In another embodiment, reports an error flag when unauthorized entities attempt to establish communication with an agent.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Service usage synchronization data	IPDR or other data that is used to synchronize the device service usage counters. In some embodiments the data is time stamped so that the service usage at a point in time may be reconciled between the local device usage count and the network based usage count, and then the local device usage count since the point in time may be used to estimate the present real-time usage count. In some embodiments, the service usage data from the device is used by the network as the actual service usage or billing data base for the device. In other embodiments, a bill by account function is included in the service usage synchronization data so that the service usage may be billed to different accounts other than a single or main user account.	Service usage synchronization is continuous with each heartbeat in some embodiments. In other embodiments service usage synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.
Service cost synchronization data	Information to reconcile a service cost estimate on the local device with a service cost count from a network based function. Similar to the service usage count, in some embodiments the service cost information is time stamped so that service cost at a point in time may be reconciled between the device and the network based function, and then a local measure of service cost may be used to estimate the present real-time service cost. In some embodiments the local service cost is determined by taking recorded billing events and looking up the cumulative cost of one or more billing	Service cost synchronization is continuous with each heartbeat in some embodiments. In other embodiments service cost synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.

FIG. 26E

	events using a service usage to cost look up data base stored locally on the device or available from a network function. In some embodiments, service cost estimation is done entirely in the network and the result is pushed out to the device UI. In other embodiments service cost estimation is done in the device based on local usage estimates and a local usage to cost lookup table.	
Available network information and roaming information	<p>Device receives available network or available roaming service provider information from a network function. The available network or roaming service information may include the potential network service or roaming service a device or user may choose to select, or the network service or roaming service the user has already selected. In some embodiments this information includes service cost information to aid the device or the user in determining the potential or actual costs of service usage while using the available network or roaming network. In some embodiments the service cost information is used to help the user in selecting the available network provider or roaming service provider. In some embodiments the available network cost information or roaming cost information is combined with a measure of expected or possible service usage to estimate how much a typical usage scenario may cost. In some embodiments, the available network information or roaming information is used to help the user estimate the present available network or roaming service charges for services used to date. In some embodiments service usage is recorded and sent to a network function that estimates the current service cost. In other embodiments the service cost is estimated locally on the device based on a service usage estimate and a service usage to cost look up function. In other</p>	<p>In some embodiments available network information or roaming information is requested by the device. In other embodiments, the information is periodically updated by the Service Controller or other network function that contains the information.</p>

FIG. 26F

	embodiments, the service cost is derived by querying the available network or roaming network billing system.	
System messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display a system messages or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include, etc.	System messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some system messages are generated in response to user input or requests. In other embodiments, system messages are generated on a regular time table or in accordance with a certain amount of service usage.
UI screen messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display user interface message or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include service usage UI, service choice UI, upgrade UI, transaction UI, marketing UI, billing UI, user identify confirmation UI, user service warning UI, user potential service tamper response request UI, etc.	UI screen messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments some user UI messages are generated in response to user input or requests. In other embodiments, UI messages are generated on a regular time table or in accordance with a certain amount of service usage.
Local agent check-in history	Logs and reports agent check-ins or self-reports that are made to a local agent integrity verification function.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Software install report	Logs and reports one or more aspects of software installs that have occurred on the device.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified. In some

FIG. 26G

		embodiments, the report is generated when new SW is installed.
Test billing event	In some embodiments the Service Controller or other network function may send or cause a test billing event wherein the device triggers a local billing sequence for the purpose of verifying that the billing sequence is properly logged, conducted and reported. The billing sequence can be related to a service usage event or sequence, a transaction event or sequence, or any other event or sequence that should result in a billing event.	In some embodiments, the test billing event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.
Test service event	In some embodiments the service Controller or other network function may send or cause a service usage event wherein the device triggers a local service usage event or sequence for the purpose of verifying that the service usage event or sequence is properly logged and reported.	In some embodiments, the test service usage event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.

FIG. 26H

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
<p>Verify service usage measure in network is consistent with expected service behavior</p>	<p>Network service usage measure is in conflict with expected service usage. Examples: traffic usage outside limits, address access outside limits, data rate outside limits, traffic shaping rules not being followed.</p>	<p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of the other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if errors persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service inspection process, or usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>

FIG. 27A

Verify service usage measure at device is consistent with expected service behavior	Device service usage measure is in conflict with expected service usage. Examples: traffic usage too high, address access outside limits, email accessed against policy.	Same as above.
Verify service usage measure in network is consistent with service usage measure at device	Device service usage measure varies significantly from network service usage measure	Same as above.
Verify service usage measure at one point in device is consistent with service usage measure at a second point in device	Service usage measure at one point in device stack that is inconsistent with another point indicates error or potential parasitic usage	Same as above. In some embodiments, the differences in service measures on the device may be used to evaluate the nature of the service usage policy implementation problem.
Verify that service policies in effect are as intended	Service policy setting queries result in settings that are different than intended	<p>In some embodiments, reset service policies and see if error persist. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition</p>

FIG. 27B

Verify presence of Service Processor agents	Agent does not respond to agent communication or query-response	<p>to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p> <p>In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify configuration of Service Processor agents	Agent configuration audit or configuration self check fails.	<p>In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the</p>

FIG. 27C

Verify billing events are reported or are reported properly		<p>error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source of error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify billing events are reported or are reported properly	Billing Agent query reveals logged billing events that have not been reported.	<p>In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service</p>

FIG. 27D

		<p>policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source of error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify network reported service usage measure are consistent with reported device billing data.	Billing agent is not properly reporting billing events for service usage, transactions, bill by account, or other billing event functions.	<p>In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service</p>

FIG. 27E

		<p>policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify device reported service usage measure are consistent with reported device billing data.	Billing agent reports are inconsistent with service usage reports.	<p>In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the</p>

FIG. 27F

		<p>appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
<p>Send test billing event through device and verify it is reported.</p>	<p>Test billing event is not properly reported by the device.</p>	<p>In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine</p>

FIG. 27G

		<p>agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis</p>
Verify device reports billing events reported from transaction servers.	Transaction server receipts do not correspond with billing events from device.	<p>In some embodiments, perform checks to determine if transaction server receipts are valid. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to</p>

FIG. 27H

		the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify activation tracking system presence, configuration or operation	Activation tracking service is not present, is not providing scheduled network activity reporting, or is exhibiting erroneous reports.	In some embodiments the response is to place the device ID, on a list of devices suspected of having activation tracking functions that have been tampered with for the purpose of central provider billing reconciliation. In some embodiments, install a new copy of the activation tracking service agent software either from a locally stored device copy or a network download. In some embodiments where authorization exists to manage device software and some aspects of service tracking, run further checks on device service integrity such as agent query-response. In some embodiments where authorization exists to manage a device access service connection, send error message to device UI, suspend device or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Verify device standing or service plan standing	No service plan on record or device not authorized	In some embodiments, if device is not yet activated with a service plan, provide UI with activation sequence. In some embodiments, if device is not authorized for service on one of the networks controlled by the Service

FIG. 271

Verify proper operation of Service Processor agents		Controller, send the UI an error message instructing the user how to proceed. In some embodiments, configure the Service Processor for the ambient service intended for that device. In some embodiments, download the appropriate Service Processor agent software that is appropriate for that device.
Check input to output relationship on Policy Implementation agent, Firewall agent. Check billing event reports to verify events are being recorded. Check application and traffic inspection tagging system correctly tagging traffic. Verify Service Processor heartbeat reports proper agent integrity self-checks, cross-checks and query/response sequences with Service Controller.		In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

FIG. 27J

Service Processor heartbeat response reports	One or more of the heartbeat reports indicate an error in operation, configuration, or tamper and error prevention system. Heartbeat function not functioning properly but device is still indicating service usage on the network.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Test service event	Service usage reporting system does not properly report test service usage event	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the

FIG. 27K

Load a fresh version of Service Processor software and perform integrity reports		<p>following actions:</p> <p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing test event to determine if the device is properly reporting billing events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Load a fresh version of Service Processor software and perform integrity reports	After fresh load of Access Control Integrity Agent, agent discovers one or more of the other agents are corrupted.	<p>Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a</p>

FIG. 27L

		<p>user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
<p>Verify Service Processor code configuration with agent self diagnosis checks</p>	<p>One or more of the agents indicates an error after running a self-check.</p>	<p>Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the</p>

FIG. 27M

Verify that device uses service only after being authorized		<p>device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
	<p>Device gains access to the network and does not check in with the Access Control Integrity Server and service measures indicate device is on the network.</p>	<p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on</p>

FIG. 27N

		<p>quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify user standing	User does not respond with proper response to UI query such as request for ID., password or biometric input. This process may be part of handling a suspected error.	<p>In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis. In some embodiments, the user may be asked to acknowledge a service coverage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service coverage acknowledgment.</p>
Agent communications log	Unauthorized communications with one or more agents is detected	<p>In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control.</p>

FIG. 270

		<p>In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
--	--	---

FIG. 27P

Service Policy Implementation Tamper or Error Protection Techniques	Example Error Trigger Criteria	Example Error Responses
Detect or block device networking activity that is potentially harmful for the operation of Service Processor.	Network activity is observed in service monitor reports that fit known patterns that indicated harmful software may be present on device.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized Service Processor software from being loaded.	Access Control Integrity Agent discovers software that is on a known malicious list.	Same as above.
Detect or block unauthorized access of protected Service Processor software or hardware memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized communication with Service Processor software or hardware.	Unauthorized communication is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

FIG. 28A

Secure loader with signed SW installed into protected memory	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor agents.	Secure communication link is in error or unauthorized access is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh agents with communication links that are in error or entire Service Processor. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor and Service Controller.	Service Processor communication is lost.	Send error message to device UI (if possible), suspend device, place on SPAN, place on watch list, place on further action list or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Execution of Service Processor software within secure memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

FIG. 28B

Storage of service processor software in secure memory	Secure memory violation or Service Processor stored in non-secure memory	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detection or removal of software thought to be harmful to Service Processor operation.	Unauthorized software is detected.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Recording and reporting of software loading signatures, software activity signatures or network activity signatures for later identification of threat sequences.	Unauthorized software or malicious network activity is detected	Same as above.
Implement critical Service Processor software as a self-refreshing program that resists corruption by running self-audit and reinstall processes such as placing audit function in inaccessible memory or OS functions or bios.	Re-installation function alerts that Re-installation has been required. Continued re-installations or failure to re-install alert increases severity of warnings.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Encrypted agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code encryption	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send

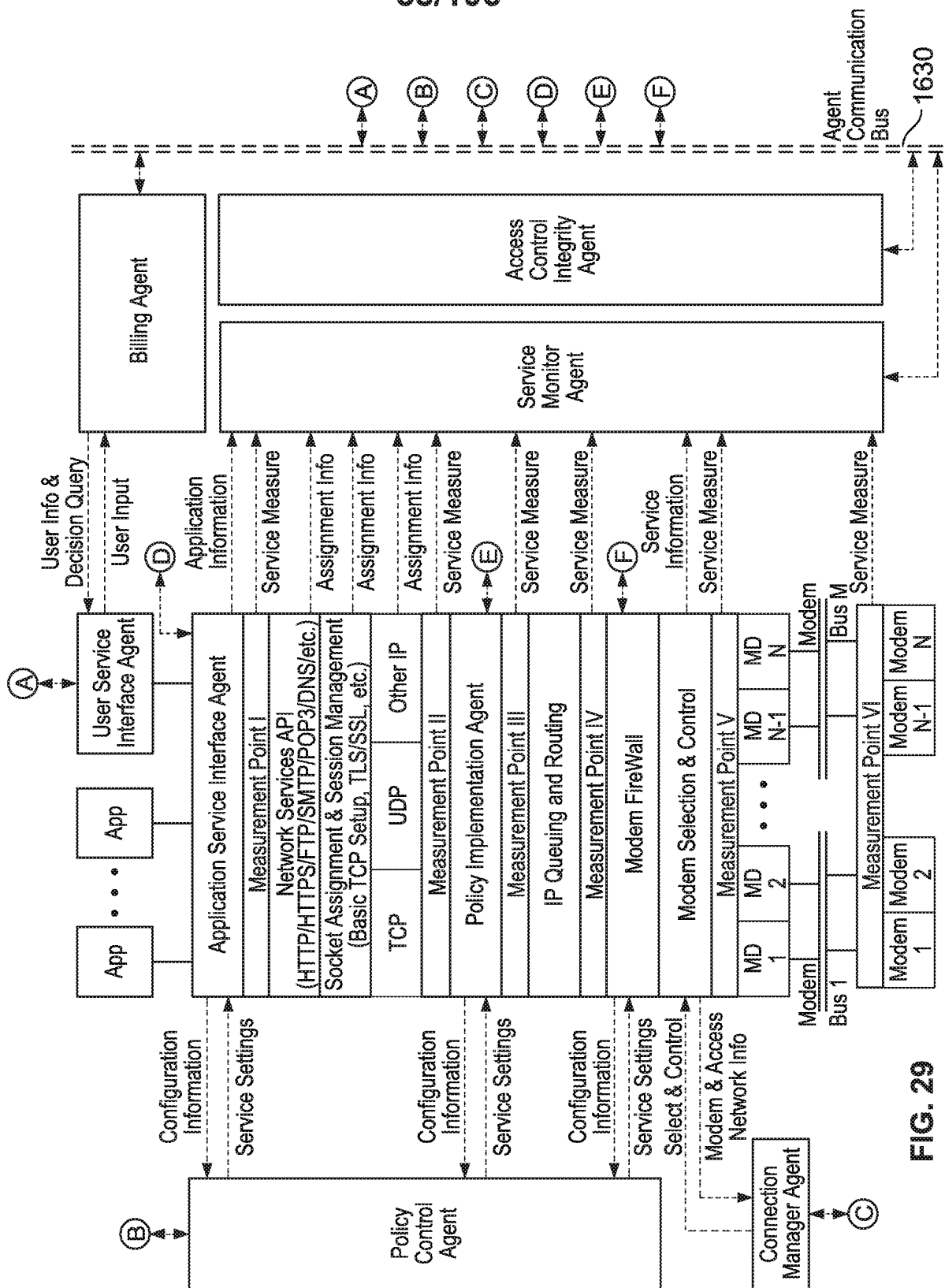
FIG. 28C

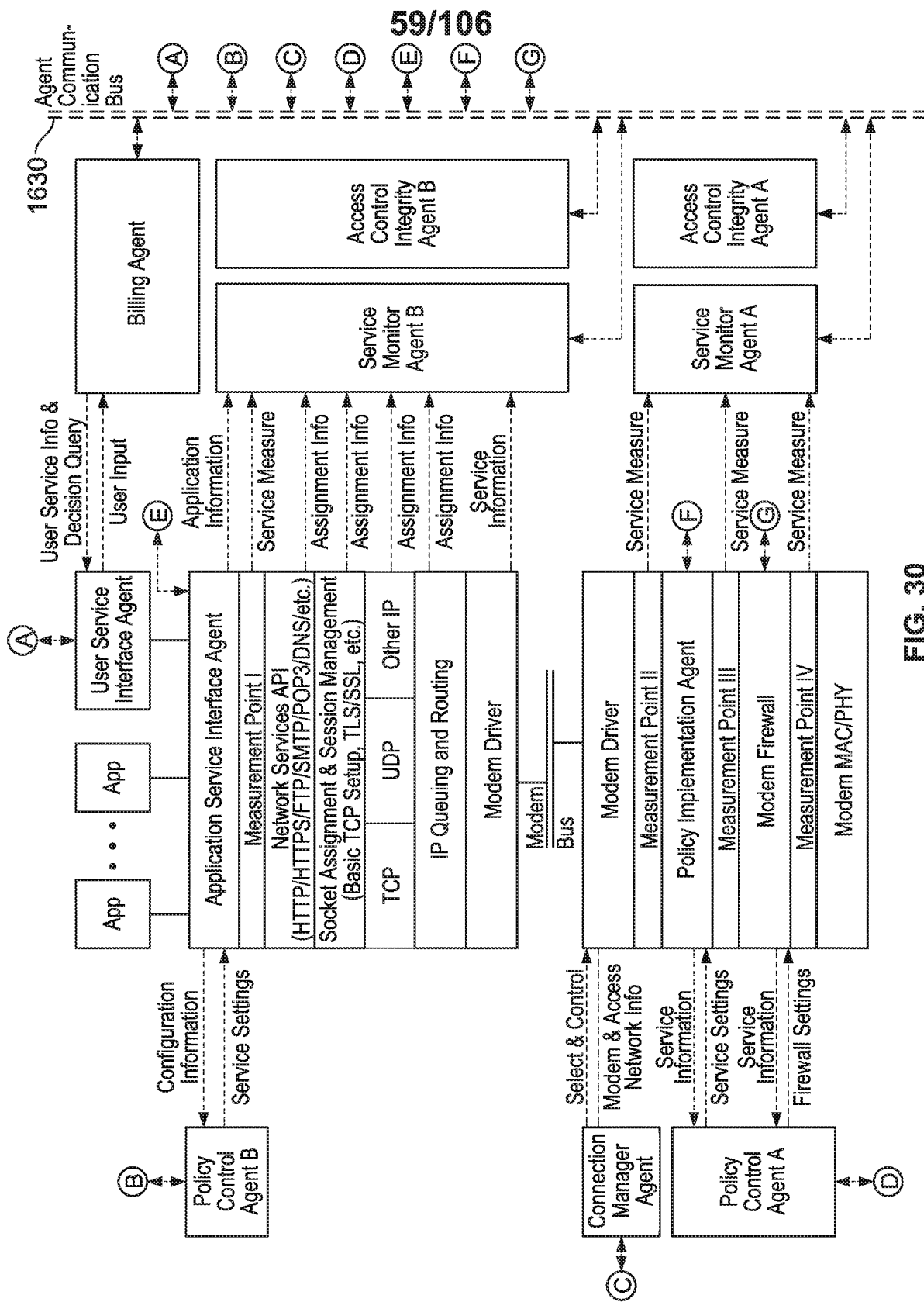
		error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Obfuscated agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code obfuscation	Same as above.
Unique agent identification numbers and signatures	Agent is discovered to have an incorrect ID, or fails signature	Same as above.
Secure agent communication bus	Agent communication bus monitoring discovers unauthorized communication or other unauthorized access to one or more agents is discovered	Same as above.
Agent level message encryption	Agent is found to be communicating without the required level of agent communication encryption	Same as above.
Service control link message level encryption	Unauthorized communication traffic is discovered on service control link	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Service control link transport layer encryption	Unauthorized communication traffic is discovered on service control link	Same as above.
Agent communication access permissions	Unauthorized communication is discovered with one or more agents	Same as above.

FIG. 28D

Agent communication log	Unauthorized communication is discovered with one or more agents	Same as above.
Encrypted agent code for downloads	Agent download is found to have incorrect or absent encryption or signature	Same as above.
Secure downloader memory	Unauthorized access to or storage in secure downloader memory is discovered	Same as above.

FIG. 28E





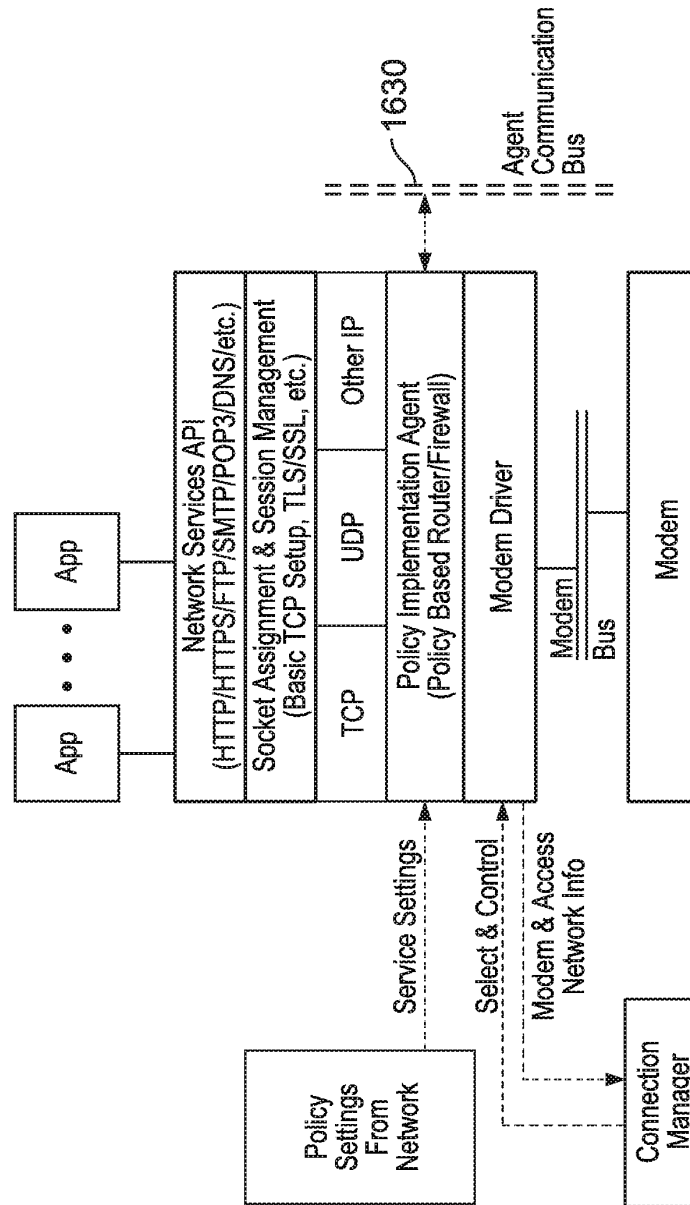


FIG. 31

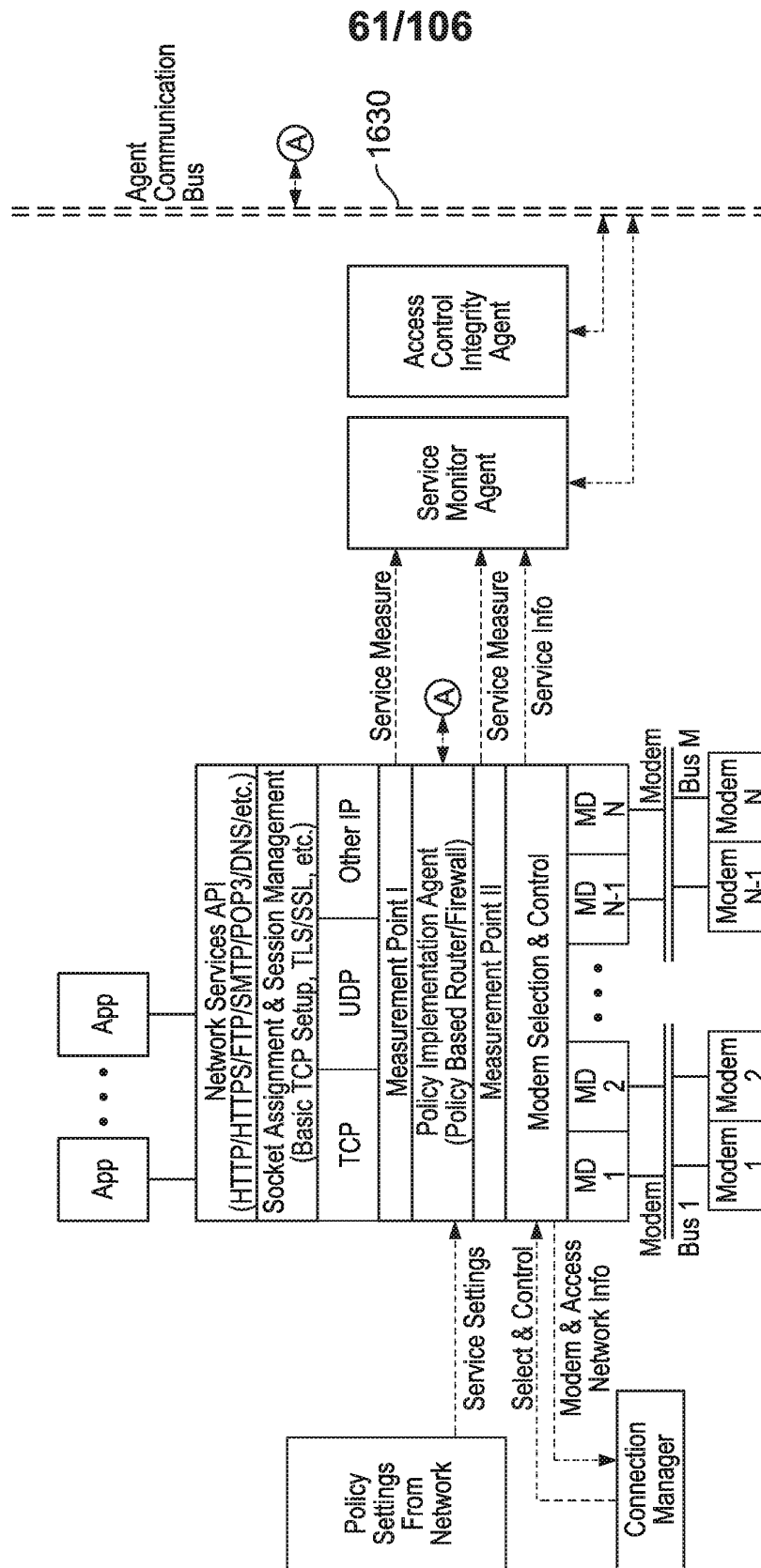


FIG. 32

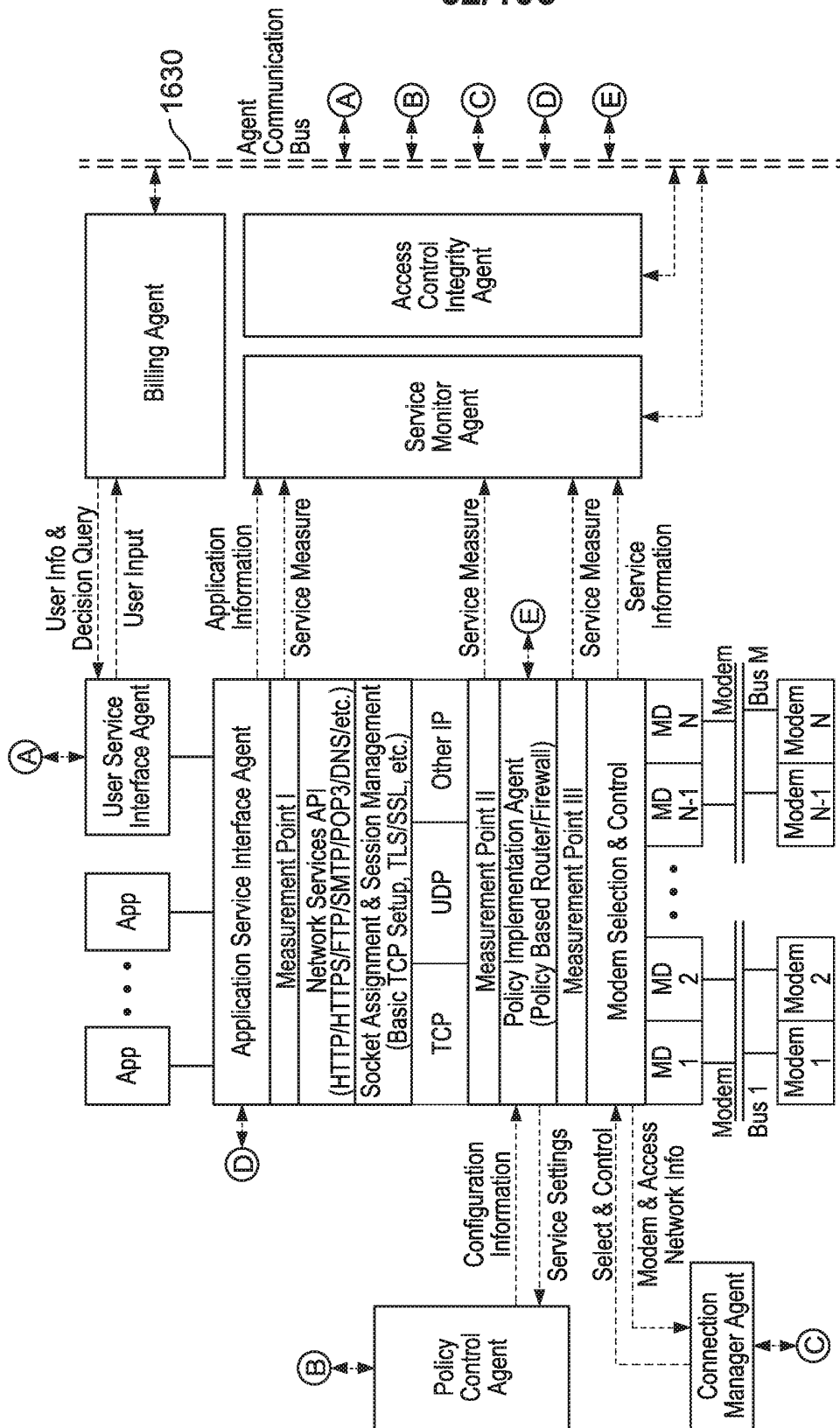


FIG. 33

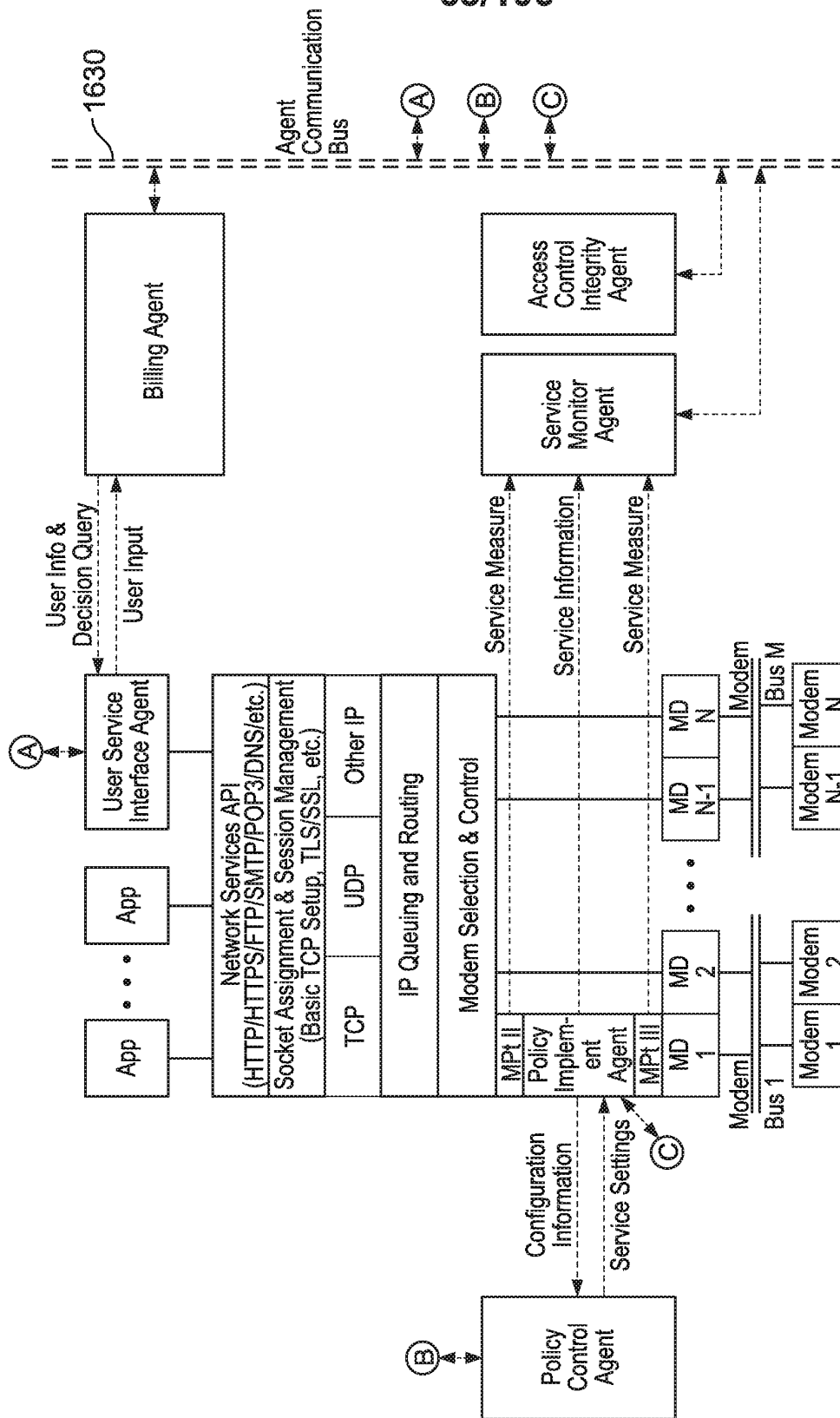
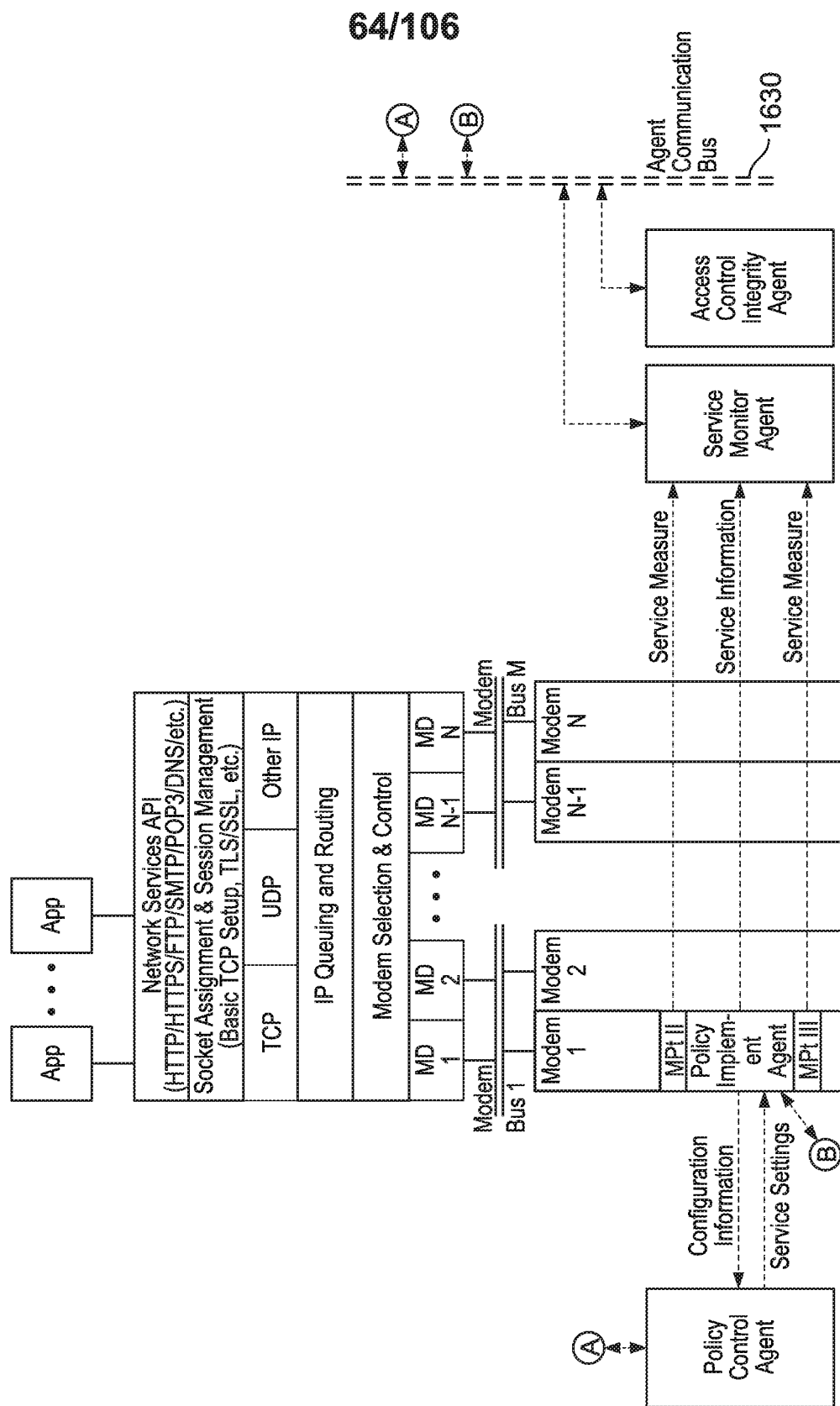


FIG. 34



64/106

FIG. 35

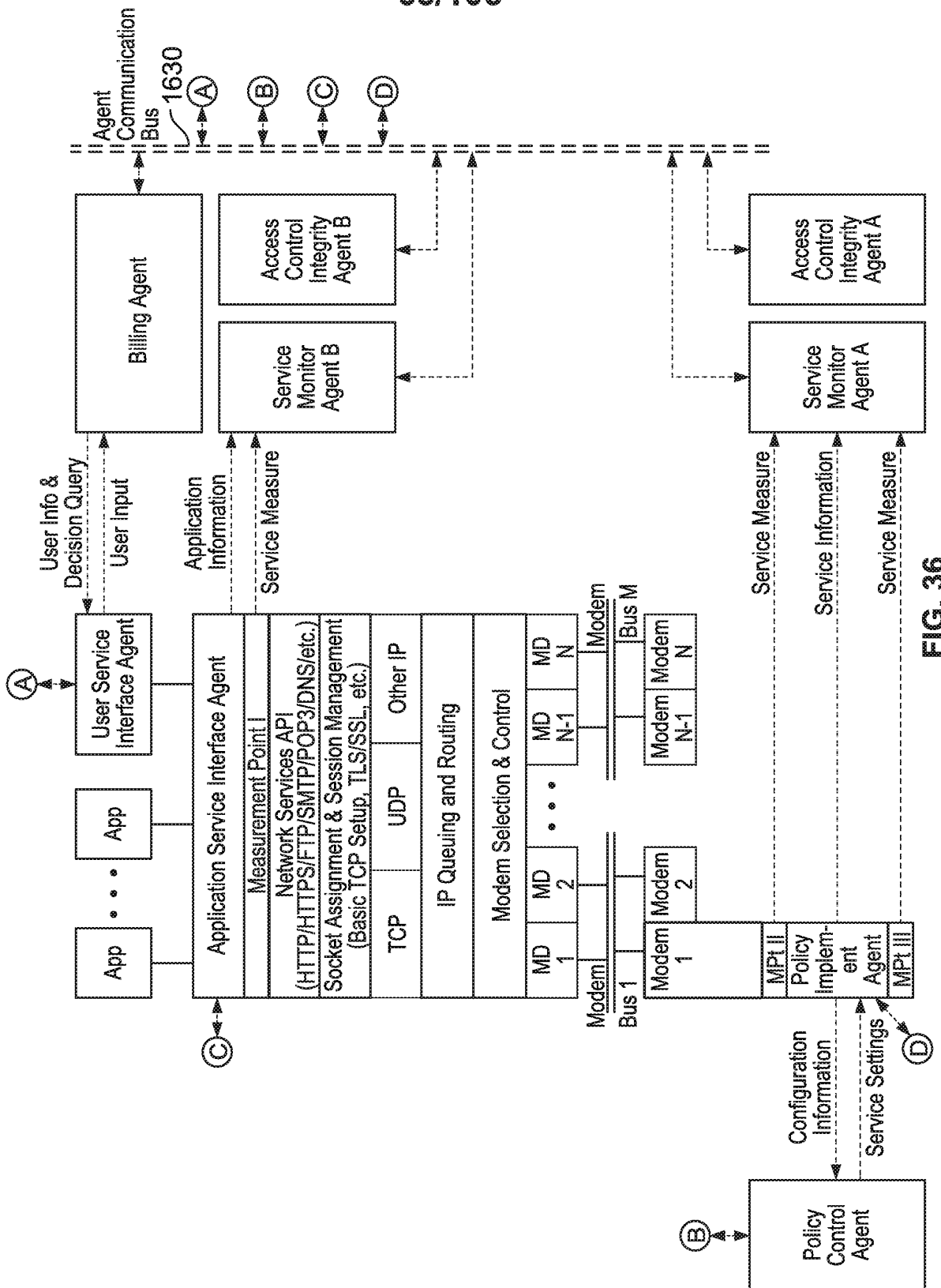


FIG. 36

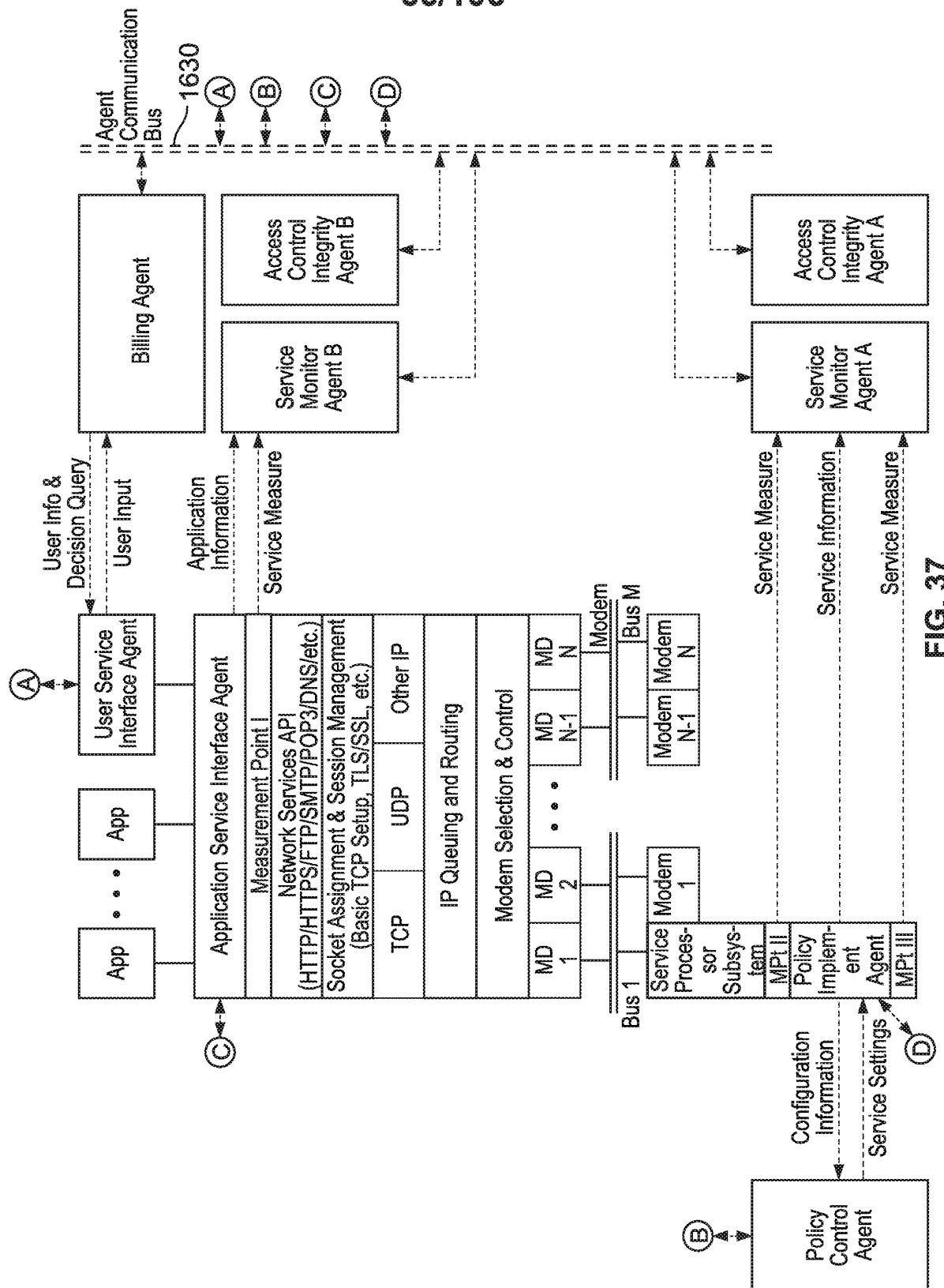


FIG. 37

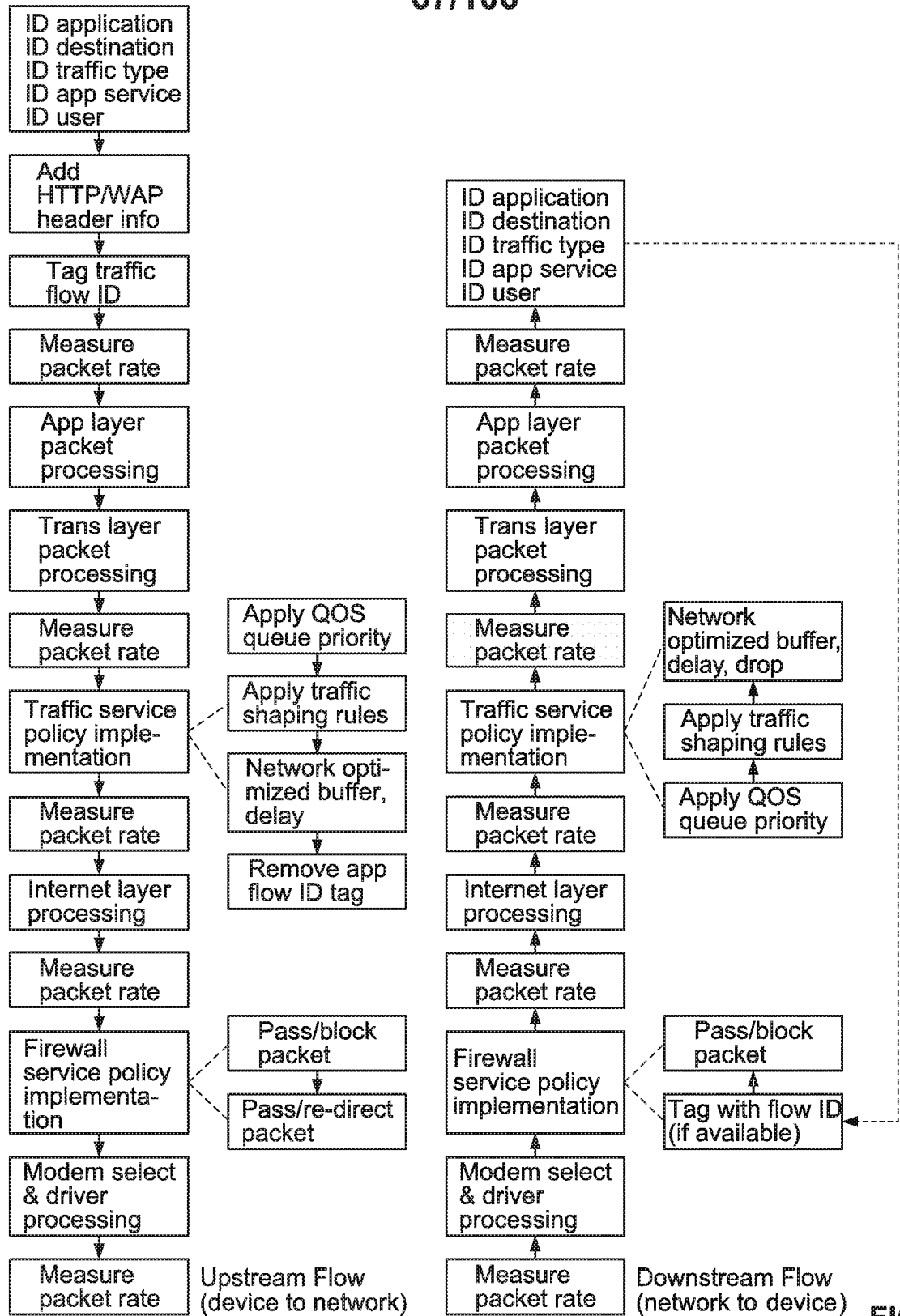


FIG. 38

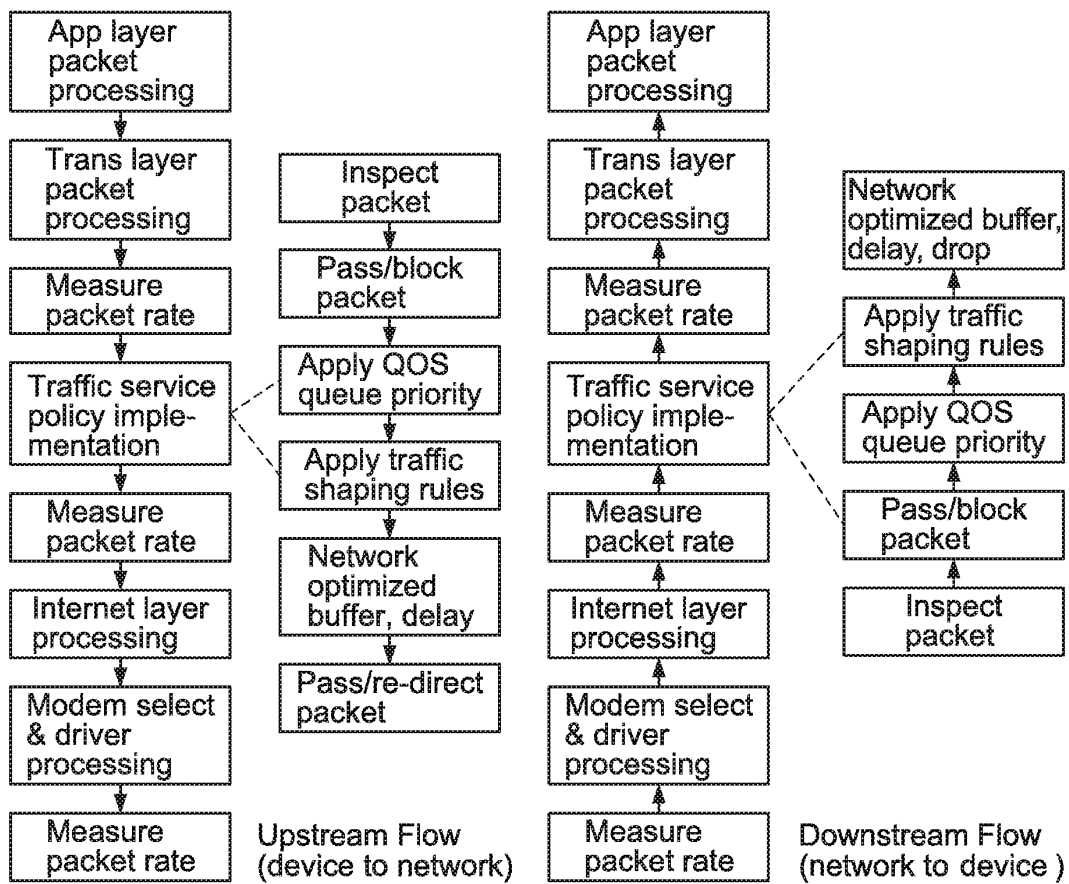


FIG. 39

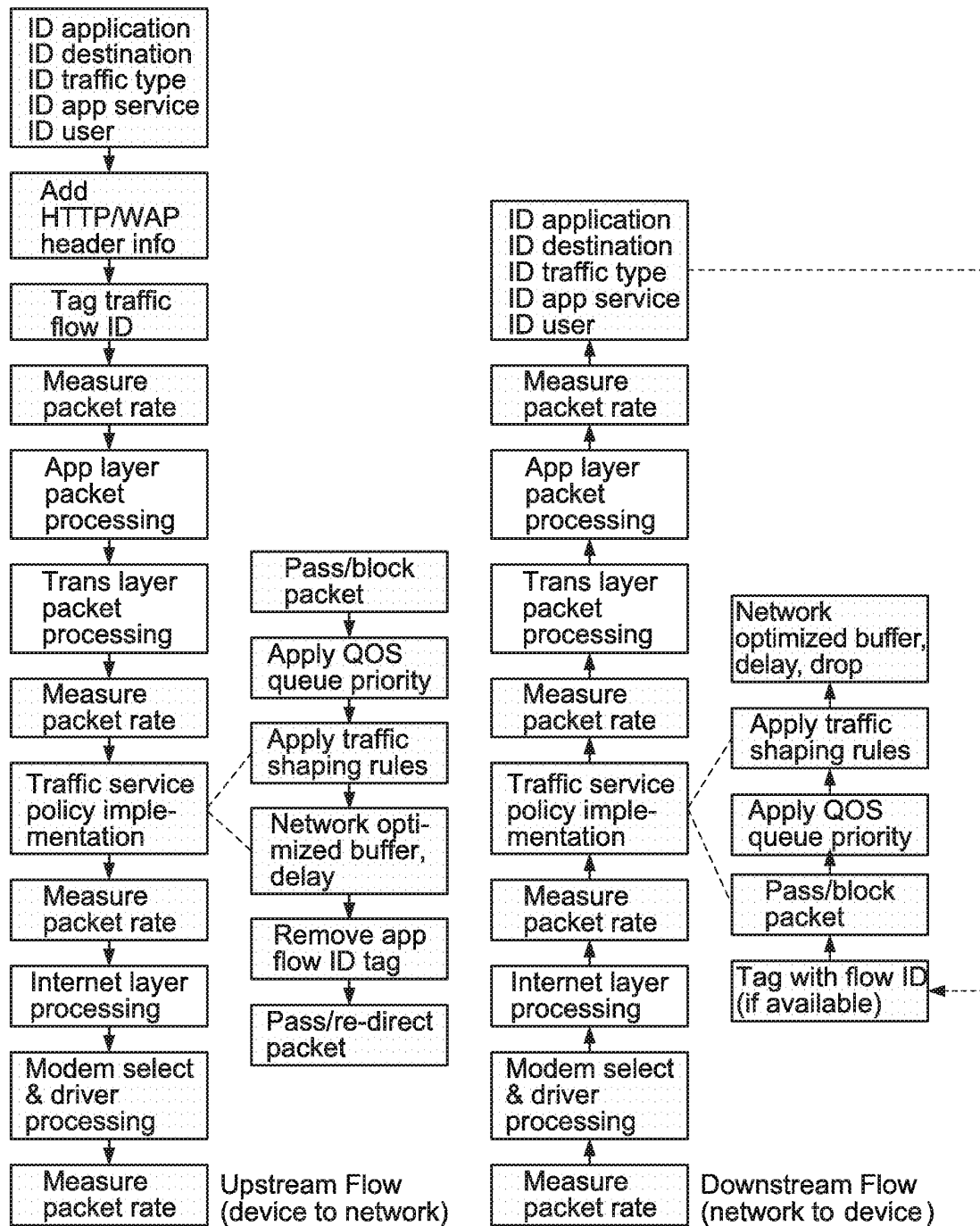


FIG. 40

Example Device CRM Data Collection and Reporting Classification	Partial Description	Example Sensitivity Level Classification	Example Authorization Level to Include in Report
Basic non-specific service usage parameters	User sensitive information is filtered from this report which is used for purposes such as service control, service control integrity monitoring or network traffic analysis.	Low	None
Service billing events or service plan selection events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with basic service agreement or enterprise agreement
Transaction billing events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with central billing agreement or enterprise agreement
Device location – customer location based service assist	Reports customer location for the purpose of assisting with location based services such as directions, yellow pages, shopping and social networking.	High	Customer authorization with basic service agreement or enterprise agreement
Device location – device or people tracking	Reports customer location for the purpose of providing tracking services for the device or the user.	High	Customer authorization with separate device tracking service agreement or enterprise agreement
Transaction associated information	Reports customer information such as networking activity, location, advertising usage, shopping behavior that is associated with a commerce transaction or happens around the same time as the transaction.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
URL history	Reports customer web surfing history.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
Served and visited advertisement history	Reports the advertisements served to the user or which advertisements the user responded to. This information may be used to determine customer preferences or for a revenue sharing relationship with the advertisers.	Medium	Customer authorization – potential service discount, perk or upgrade or enterprise agreement
911 Service usage and location trace log	This log contains all information pertinent to emergency service personnel responding to a 911 call or other emergency situation. In some embodiments this information is password protected and generally not available to the service provider unless it happens to also be contained in reports authorized by the consumer as in the examples above.	Very High	Available only for 911 support or enterprise agreement

FIG. 41

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Block Downstream or upstream traffic	Various embodiments block traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Basic authority to pass or block traffic for access control, authorization, ambient services, or plan specific services typically may be provided by the user when they acknowledge the service plan agreement. Authorization to block traffic access as part of controlling user service costs typically may be provided by the service plan agreement options the user chooses to manage cost or may be provided when the user acknowledges the limitations in the UI notifications.
Pass downstream or upstream traffic	Various embodiments allow traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Same as above.
Limit maximum data rate	Various embodiments limit maximum data rate for traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of how this command can be implemented include limiting data rate to the device according to service plan; limiting data rate by network address identifier, application or content type for the purpose of implementing a tiered garden; limiting data rate in to different levels according to the type of access technology used by the present network connection; limiting data rate to different levels according to the service provider for the present network; or limiting data rate according to an agreement or lack of agreement with a transaction provider. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

FIG. 42A

Analyze traffic	Provides capability resident on the device to analyze device or user traffic statistics to determine how to implement adaptive policy control or how best to assist the user with notification messages. In some embodiments it is important to perform traffic analysis locally on the device to reduce network chatter with the Control Processor or to maintain user CRM privacy levels by not sharing sensitive raw traffic usage history needed to determine implementation of less sensitive service control policies. Typical but non-exhaustive examples of command usage are analyzing traffic usage statistics or patterns to determine compliance with service plan limits; analyzing traffic usage statistics or patterns to determine likely future compliance with service plan limits; analyzing traffic statistics or patterns to categorize usage according to network address identifiers, applications, content types, network types or central providers; analyzing traffic demand vs. usage statistics or patterns to determine if user may be better served with another service plan; analyzing traffic statistics or patterns to identify potential tamper threats. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode, but adaptive application of the analysis results is typically associated with adaptive policy control mode.	Authorization to analyze traffic for local device service policy control purposes or 911 service typically may be provided for in the basic service contract. Authorization to transmit a complete or filtered version of the traffic analysis to the Service Controller typically may be provided under user selected options in the service plan contract.
Successive limitation	Provides capability to begin with one limit on access or data rate according to a set of defined service usage trigger criteria, to further limit access or data rate according to said criteria, and then to successively remove limits according to said criteria. In some embodiments this function provides for service usage that starts at a given level for one or more service aspects, but as said service aspect exhibits usage that potentially threatens an overage on service plan limits then the level of service for said service aspect is reduced successively until the threat of service plan overage is reduced or eliminated. In some embodiments, the limits on service level for said service aspect are eventually removed either all at once or successively over a specified time period or set of time periods so that the limits on service level for said service aspect are eventually removed if the service aspect is used less vigorously for a period of time. In this type of embodiment the projection for future service usage by a given service aspect is assisted by the analyze traffic statistics function. As a more specific example, the service aspect may be a URL address that is popular with the user and demands a high service consumption, and the data rate allowed to that URL may start at a relatively high level when the user first begins to surf and as long as the surfing session is finished quickly there is never a reduction in service level, but if the user surfs for a longer time so that service usage begins to threaten plan limit overage, the data rate allowed to that URL is successively reduced the longer the surfing session occurs. Continuing this	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

FIG. 42B

	<p>example embodiment, if the URL is not visited for a defined period of time then the data rate limitation may be removed in steps over multiple pre-defined time periods, or may be removed all at once back to the initial data rate established in the service policy for that URL. Other specific embodiment examples include email download or upload data rate; download or upload rates for certain types of file transfers; or download or upload rates for a given network access technology or central provider. This command is associated with adaptive policy control mode for the Service Processor. In more advanced adaptive embodiments, the policy control system first identifies those service aspects that are consuming a large percentage of the service usage and then begins to successively limit service level only for these highest usage service aspects so that all other service aspects that are not responsible for potential service plan limit overage continue to receive relatively high service levels. In another embodiment, some high usage service aspects may be exempt or partially exempt from limitations in service level, as for example a service aspect that is associated with a secondary source of service or transaction payment or that may be separately accounted for in the service plan usage reporting.</p>	
Limit email file transfers	<p>Sets and enforces limits on email downloads. In some embodiments this can include use of the successively limit functionality. In some embodiments, this is accomplished by identifying specific email downloads or uploads and controlling traffic for those traffic flows. In other embodiments, this includes interacting with the email application to set download or upload file settings. This functionality may be implemented in instantaneous policy implementation mode or adaptive policy control mode, with the more advanced functionality such as successive limitation on email file transfers being implemented in the adaptive policy control mode.</p>	<p>Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.</p>
Seek to manage below service limit	<p>Implements adaptive policy control in an attempt to manage service usage to reduce service plan limit overages. In some embodiments there are successive limits on service level for overall traffic, or for the highest usage service aspects, with the successive limits being lowered until average service usage is projected to be below service plan limits. The algorithms that may be applied to achieve this adaptive service level limitation are quite varied and only a few are given here. In one embodiment, the service usage for the service plan period is projected using the analyze traffic functionality, and overall device data rate is successively limited until service usage is projected to be below the service plan limit. In another</p>	<p>Same as above.</p>

FIG. 42C

	embodiment, the analyze traffic functionality is used to identify those service aspects that are causing the majority of the service plan usage, and then each of those service plan aspects are limited using the successive limitation functionality, with the service level limitations being based on the traffic usage patterns and specific application scenarios for each service aspect. For example, in some embodiments the service aspects that are creating the most service usage are subjected to more service level limitation than service aspects that are creating less service usage. Service usage may be defined as usage of a raw service measurement such as total data consumption, files downloaded or time spent on network, or it may be translated into an economic measure using the lookup service cost functionality. In some embodiments, the period of time elapsed in the service accounting period is taken into account in determining...	
Synchronize service usage counters	Synchronizes service usage counters on device from time to time to minimize service accounting errors between the device data base and the central billing data base. In some embodiments this is a part of the Service Processor heartbeat communication system that need not happen every heartbeat. In some embodiments this occurs with a request for update by the device to the central billing system or to a server function in the Service Processor	Provided for in the basic service agreement.
Lookup service cost	Provides a data base of service usage vs. cost for each type of service offered on the device. Provides for a lookup function of service cost.	Same as above.
Convert service usage to service cost	Uses the service cost vs. usage lookup function to transform one or more service usage aspects to one or more service cost aspect. One example embodiment provides a service cost measure for one specific aspect of service usage, for example total data consumed over a period of time. Another example embodiment provides a total service cost measure for all service usage over a period of time.	Same as above.
Notify user of service overage	Sends a notification message or screen to the UI to inform the user that the one or more aspects of service usage has exceeded the specified limits of one or more service plans. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Same as above.
Project service usage	Uses the analyze traffic functionality and projects an estimate of what the traffic usage will be at the end of a service plan measurement interval if the service usage does not change. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above

FIG. 42D

Notify user of service cost overage	Performs a service cost estimate based on one or more aspects of service usage and informs the user that the one or more aspects of service cost has exceeded the specified limits of a service plan. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Provided for in the basic service agreement.
Notify user of usage behavior likely to run over service usage limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, notifies the user if the projected usage is over the service plan limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Notify user of usage behavior likely to run over cost limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user if the projected cost is over the service plan cost associated with the service plan service limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Project user service cost if usage behavior continues	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user of what the projected cost will be if the service usage behavior remains the same. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.

FIG. 42E

Limit access likely to cause overage and notify	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, if the service usage is projected to go over the service limit, notifies the user that limits are being applied to keep service usage or cost under the service limit, applies limits to various aspects of service usage to bring down usage so that projections are within service limits. In one embodiment, the seek to manage below service limit functionality is used.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Require acknowledgment of notification	Requires the user to acknowledge a notification of potential service or cost overage or a notification of an option to limit the service overage or cost of service overage.	Provided for in the basic service agreement.
Log or report acknowledgment of notification	In some embodiments, the user acknowledgment of notification is stored, or sent to the Service Controller, or stored and later sent to the Service Controller.	Same as above.
Notify user of service plan options prior to running over service usage limit	Notifies the user of options to extend the service plan limit before reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Notify user of service plan options after running over service usage limit	Notifies the user of options to extend the service plan limit after reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Time of day variations	Each of the functionalities for traffic control, service cost, service limits may be modified with a time of day variation so that the values used are different for different times of day.	Same as above.

FIG. 42F

Access control enable list	List of service usage activities that are enabled.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the control data base.
Access control block list	List of service usage activities that are blocked.	Same as above.
User service control option UI	Provides the user with a list of options for how they would like to control service usage or service cost.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.
User service notification option preference	Provides the user with a list of options for how they would like service notification information to be displayed. In some embodiments provides the user with the option to turn off one or more aspects of service notification. In some embodiments the user is not allowed to turn off notification for service usage events that require user decision or acknowledgement.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.

FIG. 42G

User CRM or service usage monitoring filtering option preference	Filters the device and/or user information that is being collected before it is reported to the network to maintain the desired level of user privacy. In some embodiments the user defines preferences on user privacy that are used to define the filter settings.	In some embodiments this is not accessible by the network and only may be modified by the user. In other embodiments it may be read but not written by the network and in this case authorization is restricted to service controller, VSP or other network function with proper credentials to access the filter settings data base. In some embodiments the network is allowed to change the CRM filter settings and in this case Authorization restricted to service controller, VSP or other network function with proper credentials to access the CRM filter settings data base.
Service usage billing event record	A record of service usage billing events. In some embodiments this record is transmitted to the billing server or another network function to aid service billing or billing reconciliation.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Bill by account	The bill by account embodiments provide for service billing to accounts different than the main user account, for example tracking network device chatter that is not desired to be billed to the user, transaction partner access costs that are shared with or billed to the transaction partner, ambient service cost tracking, tracking temporary account costs, etc.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Central billing transaction and event recording	Billing event tracking and reporting associated with the central provider open billing embodiments. Some embodiments include generation of billing certificates or receipts. In some embodiments the device may serve as a billing feed.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Service owner registration or re-registration	Function that allows a portion of the device credentials to be programmed to indicated the VSP.	In some embodiments authorization to write the device is restricted with security signatures or other security methods to the VSP and possibly the central provider. Some embodiments involve provisions to report to a network function when the VSP settings are changed or the software is uninstalled. Other embodiments involve restoring VSP settings or software if removed.

FIG. 42H

Credentials swap	Function that provides for swapping of credentials, for example temporary credentials to permanent credentials.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the credentials data base.
Account information swap	Function that provides for swapping the account information, for example temporary account to permanent account.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the activation service profile data base.
Configure or re-configure service processor for new device service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Ambient service profile definition	Function that provides for service processor programming for all the information that defines the ambient service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the ambient service profile data base.
Analyze service usage statistics	VSP function to analyzer service usage statistics for a device, defined group of devices, defined group of service plans or service profiles, defined group of users or other groupings.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Dry lab test new service policy	Allows simulated testing of draft service profiles and/or service plans against device usage statistics for a defined group of devices or users or service profiles, or against simulated device service usage behavior. Some embodiments show the estimated profitability of proposed service profile and service plan. Some embodiments allow decomposition of the service usage statistics to identify the user group service usage activities that may be modified by changing the service usage control policies or made more profitable by changing the service plan billing policies.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Beta test publishing system	Function that provides for service processor programming for all the information that defines the service profile device credentials, VSP and other necessary parameters for a beta test device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Publish new service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters for a production device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.

FIG. 42I

Roaming selection service	Function that surveys available roaming service partners, looks up the billing rates for the partners, and displays to the user the set of choices and billing rates. In some embodiments the roaming partner billing rates for one or more roaming partners are applied to a typical user service usage scenario for the purpose of estimating possible projected roaming costs and displaying those costs to the user. In some embodiments the roaming data is stored locally on the device and periodically updated with network refreshes, while in other embodiments the data base is looked up at the time of service. In some embodiments, the user is asked if they would like to modify their service usage notification or control profiles to save roaming costs and if the user responds yes they are provided with a set of options for changing service usage notification or service usage control policies.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the roaming service.
Roaming usage count	Provides a service usage estimate to the user while roaming.	Same as above.
Roaming cost service	Provides a service cost estimate to the user while roaming.	Same as above.
Roaming policy control service	Provides the user or VSP with the capability to switch service usage notification or service usage control policies while roaming. Some embodiments provide for restrictions to roaming carrier options. Some embodiments provide policies based on carrier chosen. Some embodiments provide policies based on the service cost for carrier chosen. Some embodiments specify preferred roaming lists that may be different than the central provider roaming list.	Same as above.
Switch policies for new network	Provides the user or VSP with the capability to switch service usage notification or service usage control policies depending on which network the device is connected to. Some embodiments provide for restrictions to certain network options. Some embodiments provide policies based on network chosen. Some embodiments provide policies based on the service cost for network chosen. Some embodiments provide for a network connection preference list.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the network selection policies.

FIG. 42J

Service
Processor
Authorization

81/106

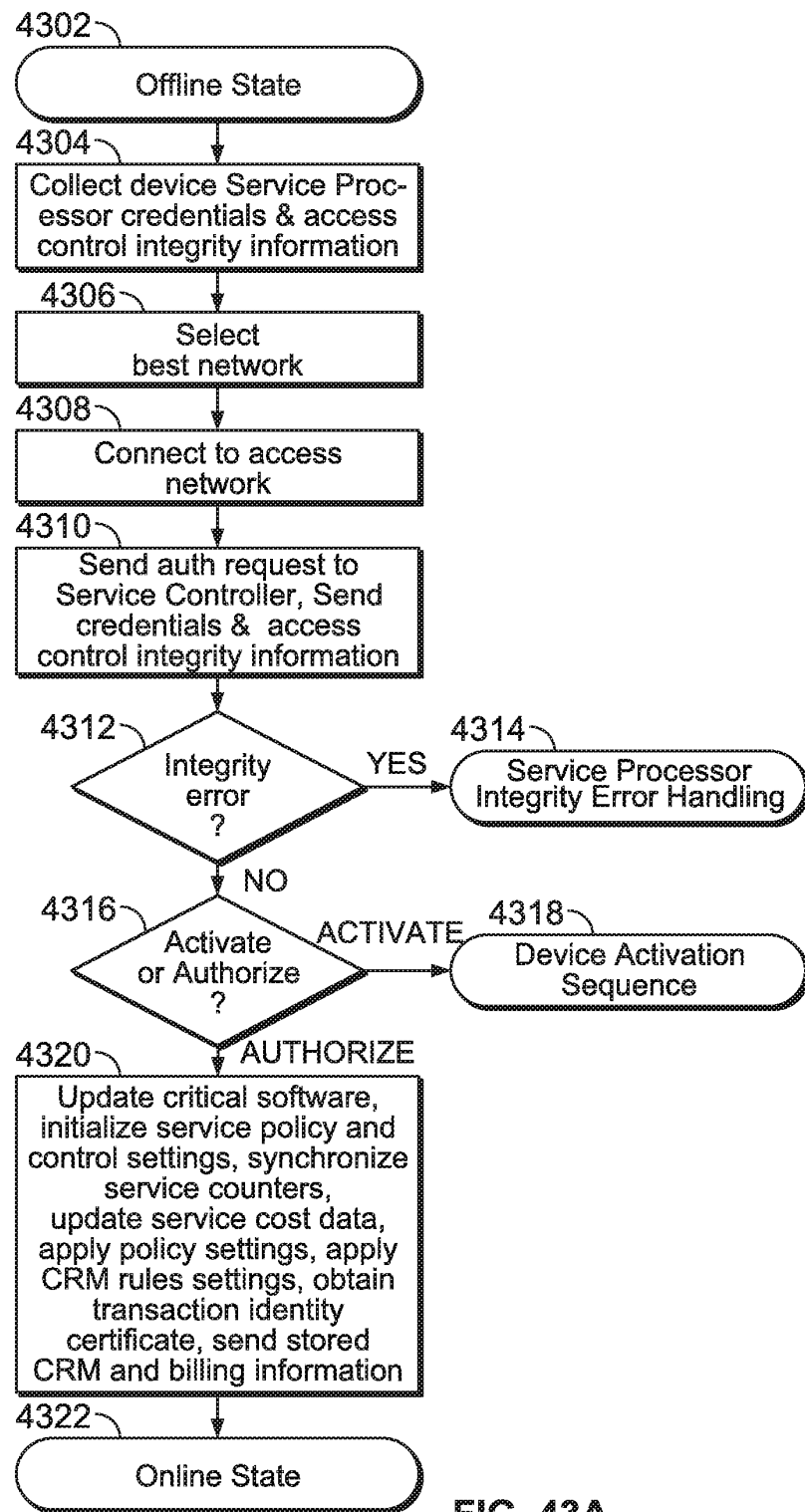


FIG. 43A

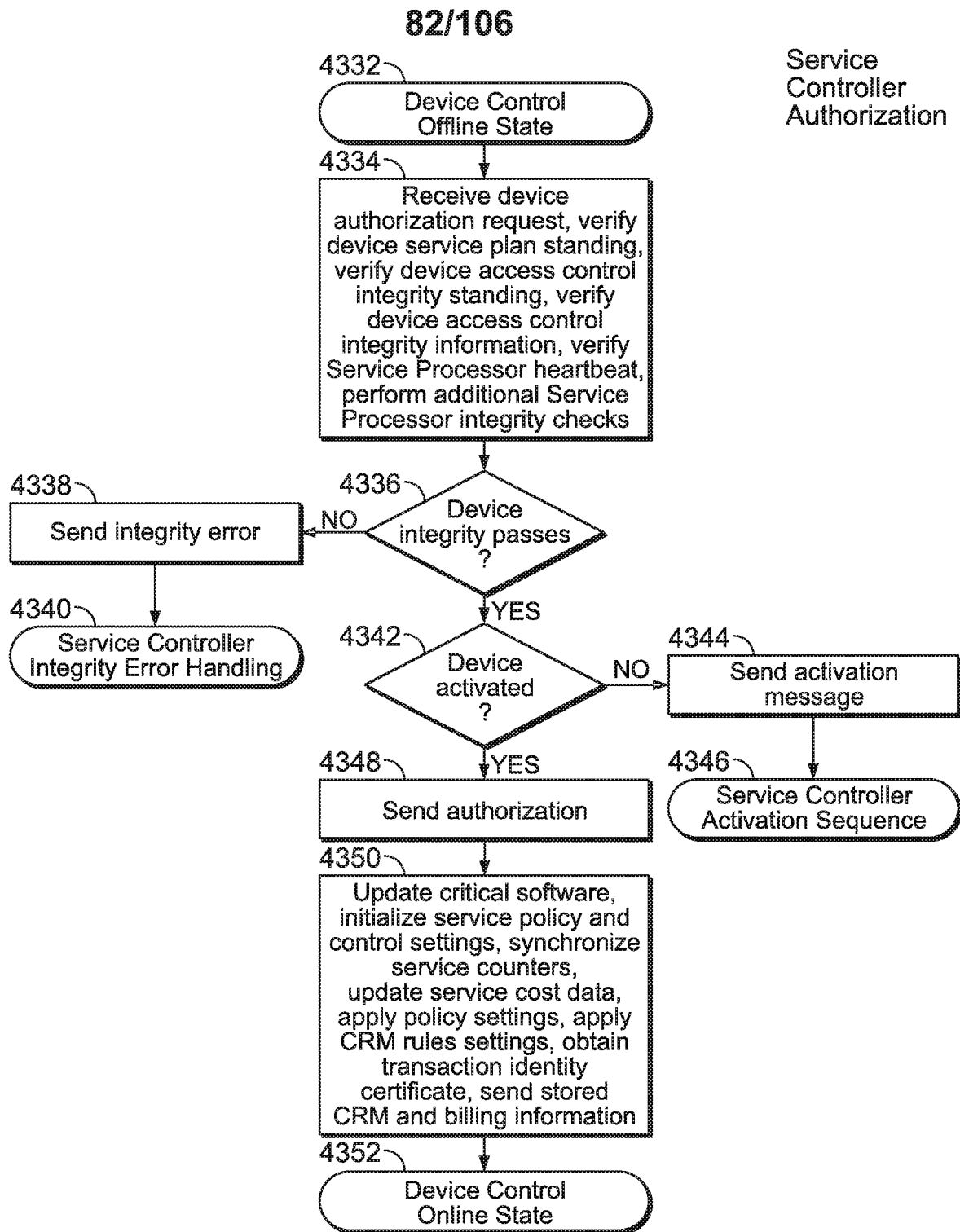


FIG. 43B

83/106

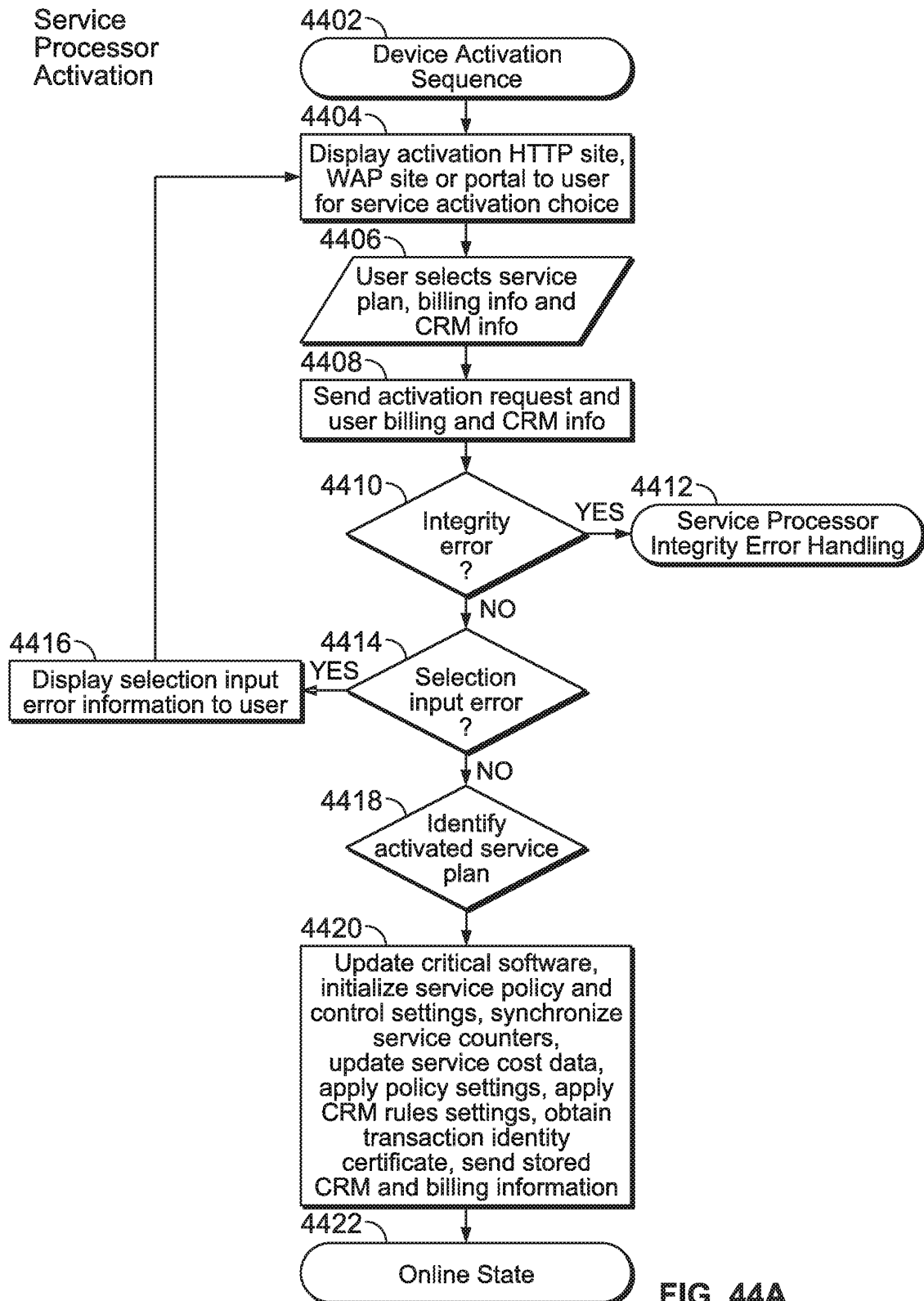


FIG. 44A

84/106

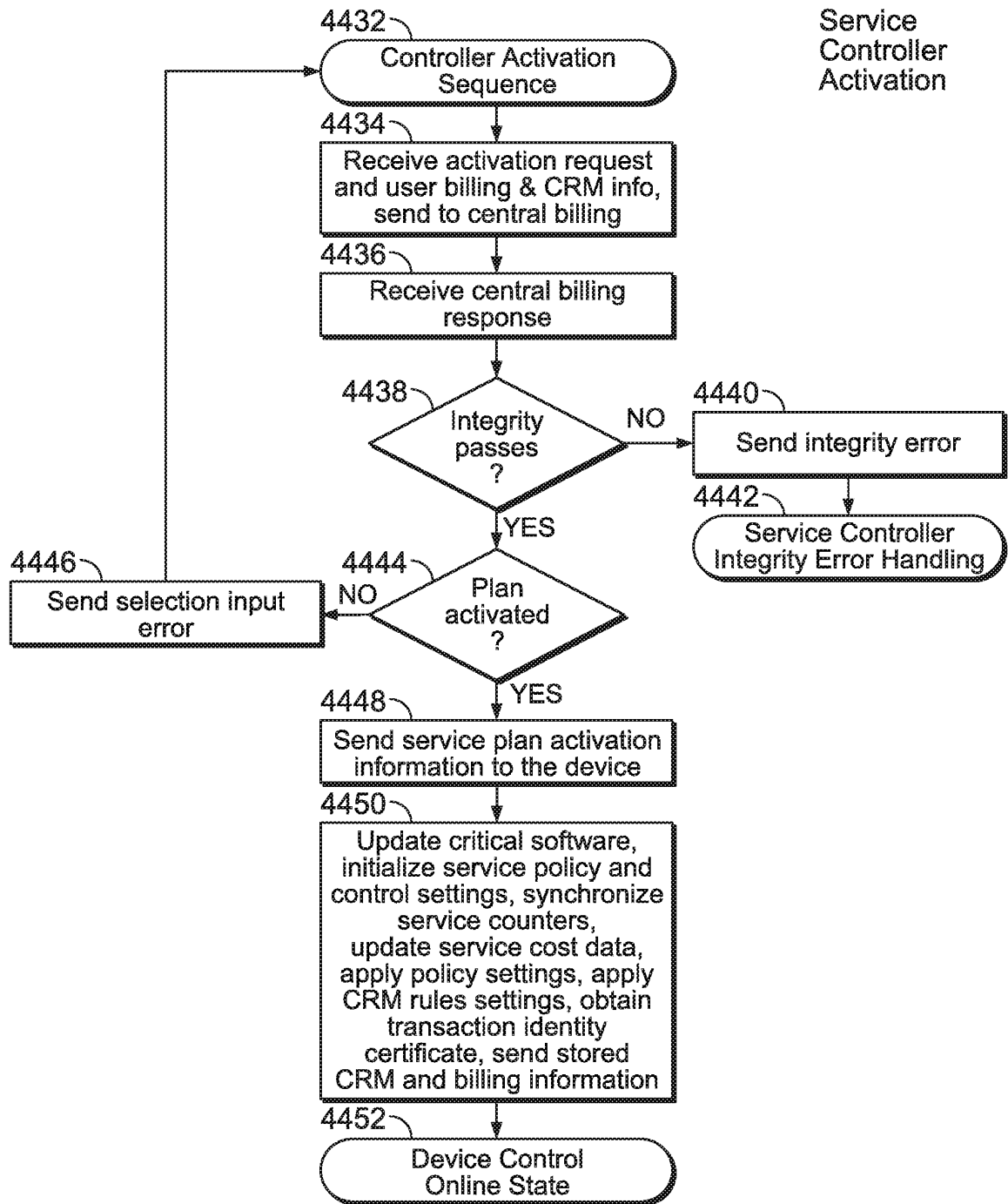


FIG. 44B

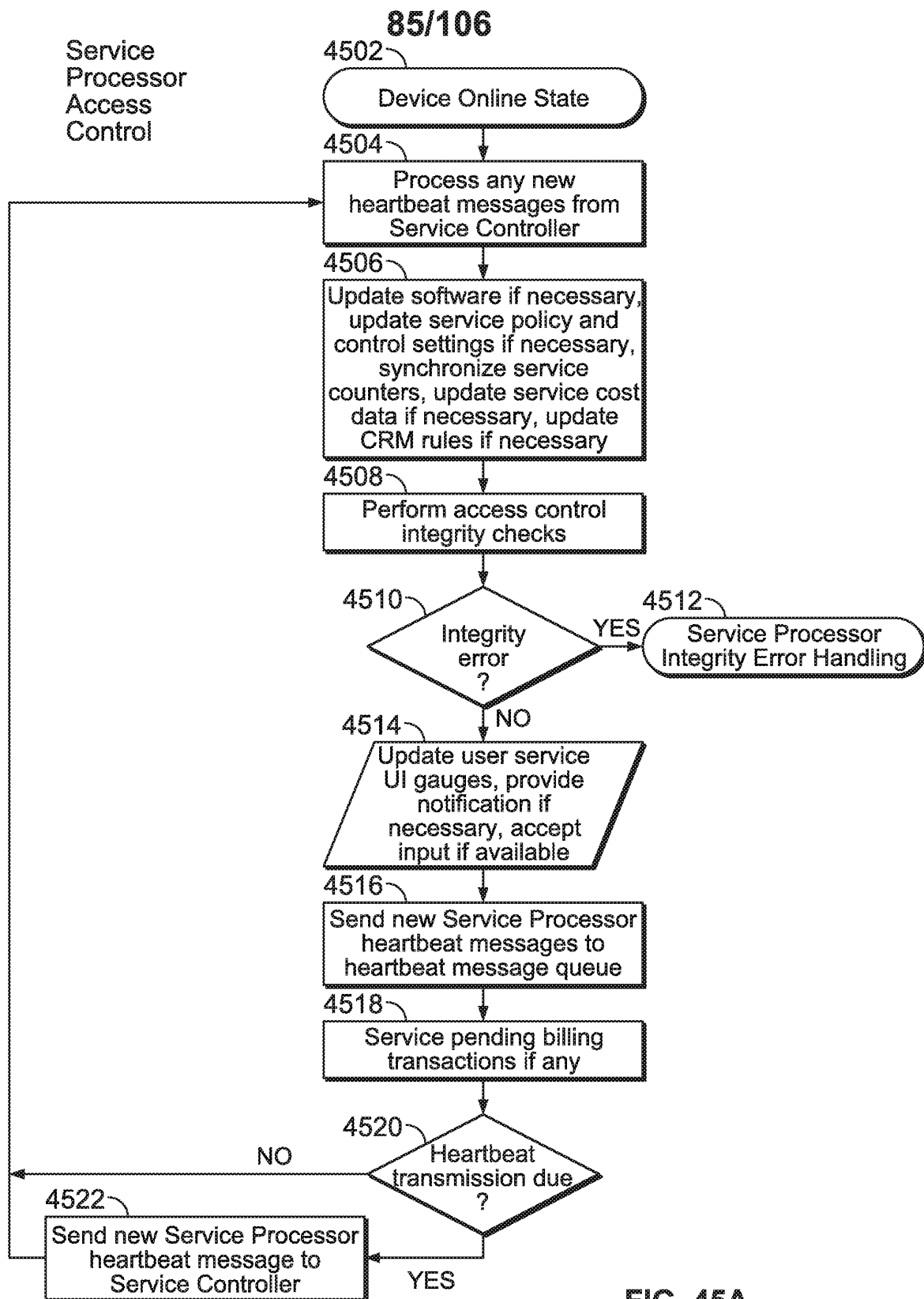


FIG. 45A

86/106

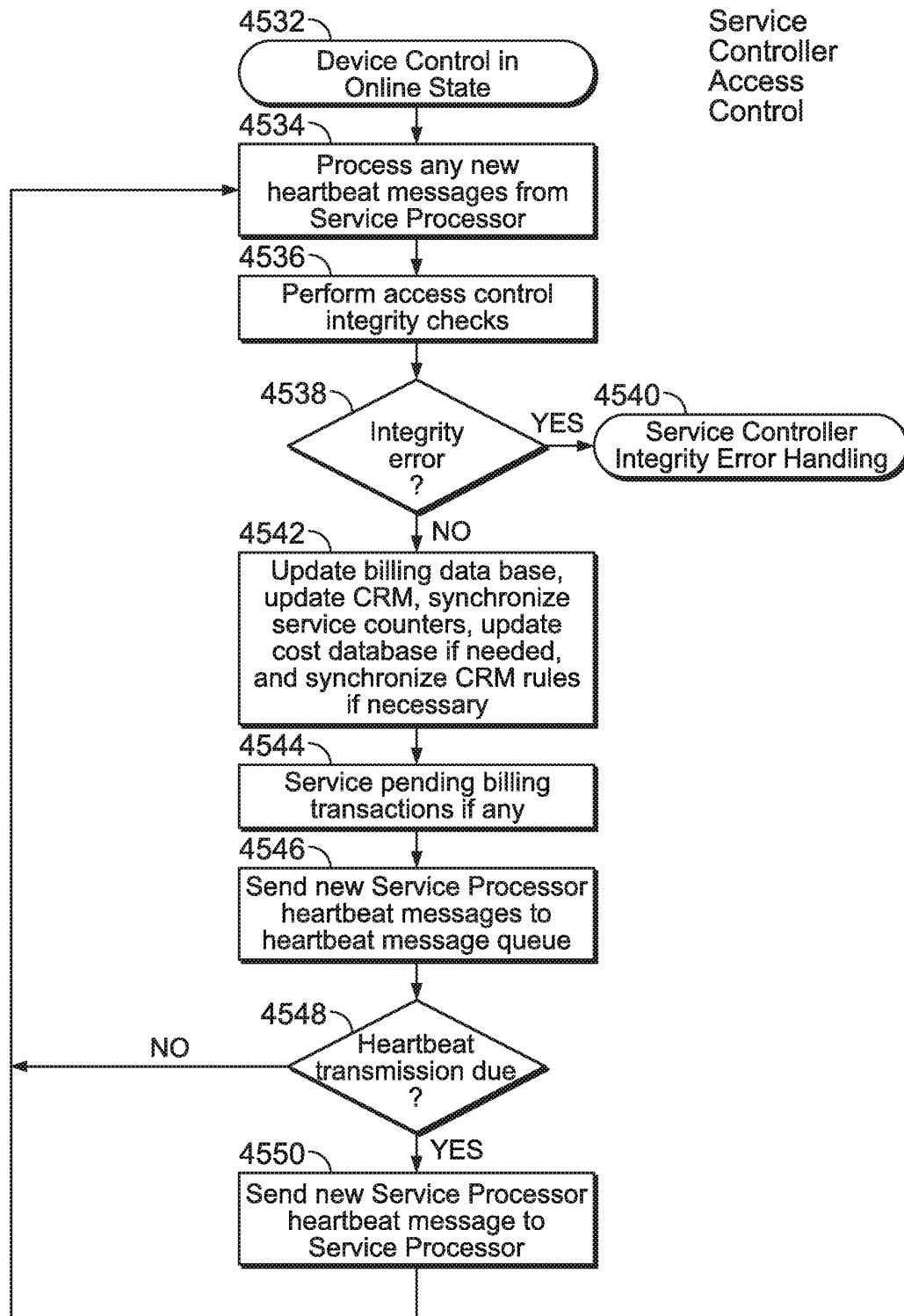
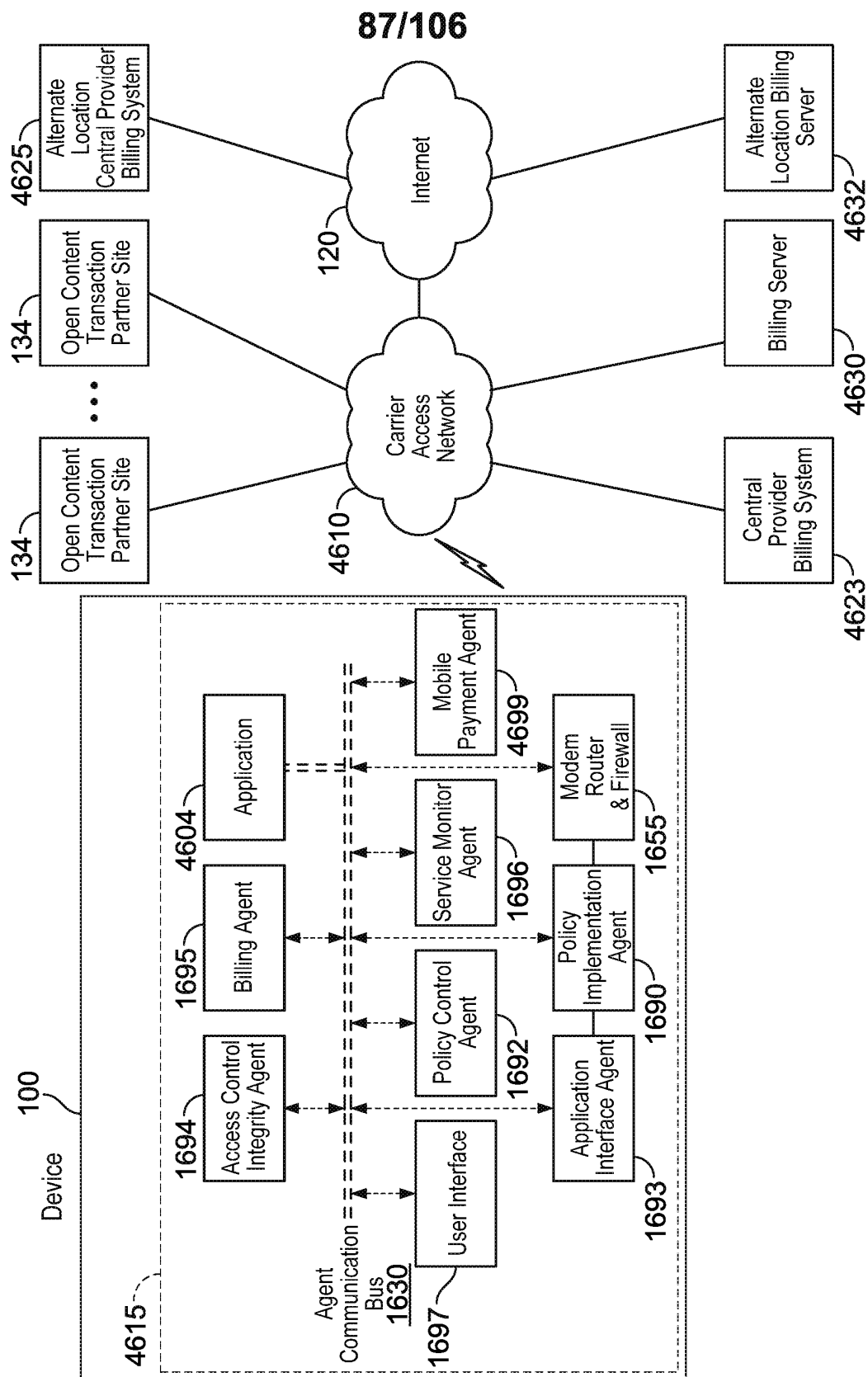


FIG. 45B



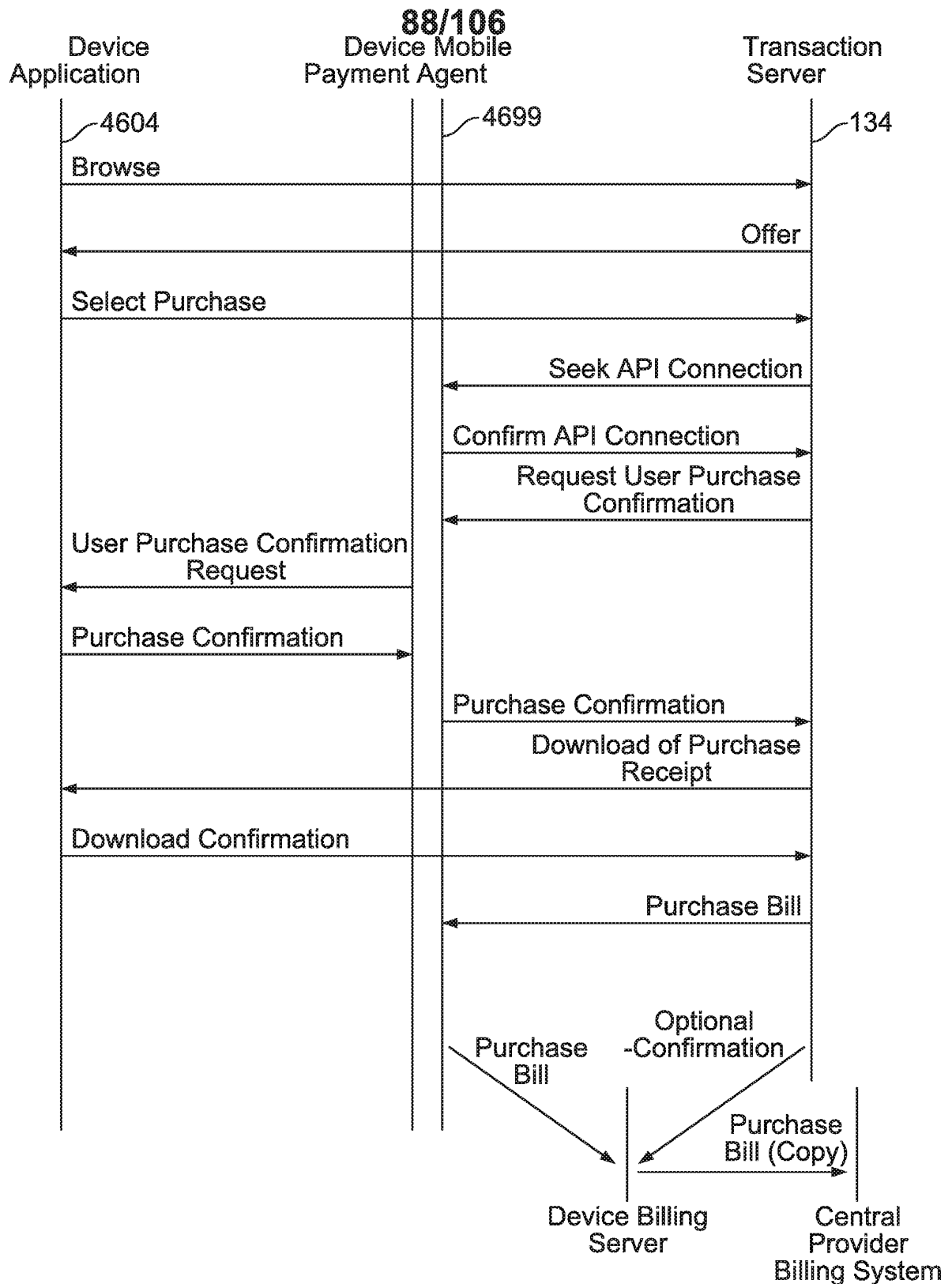


FIG. 47A

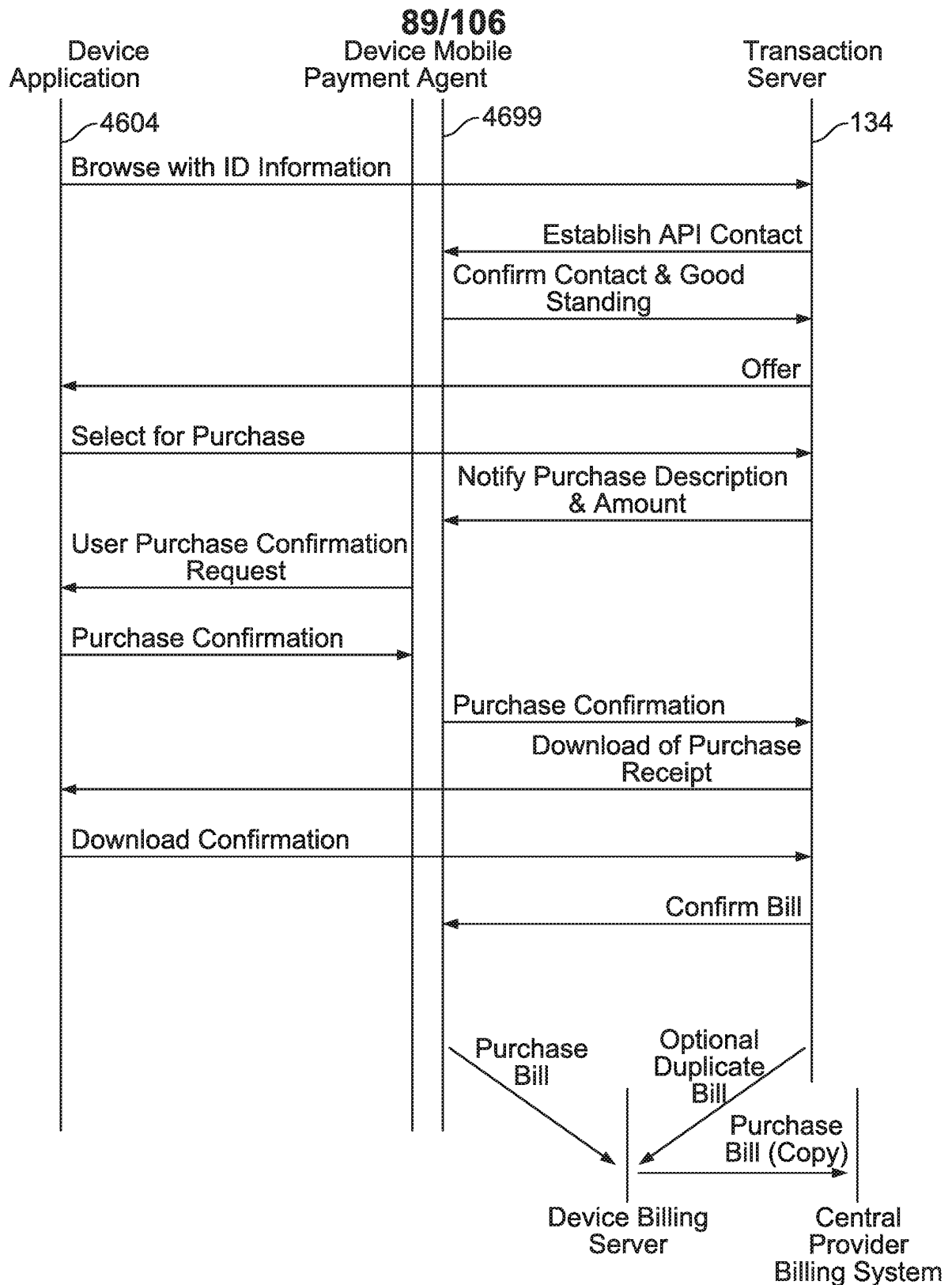


FIG. 47B

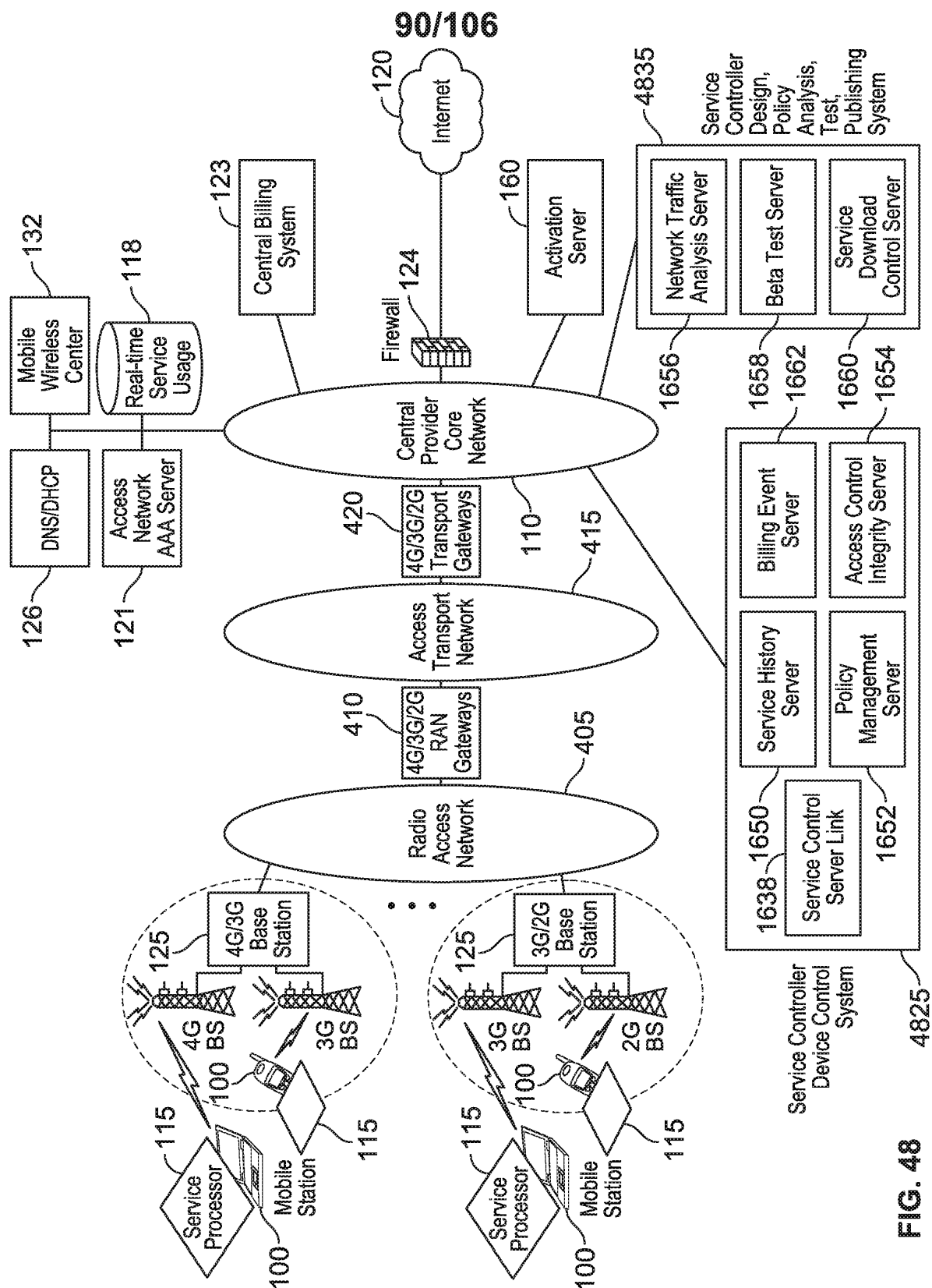


FIG. 48

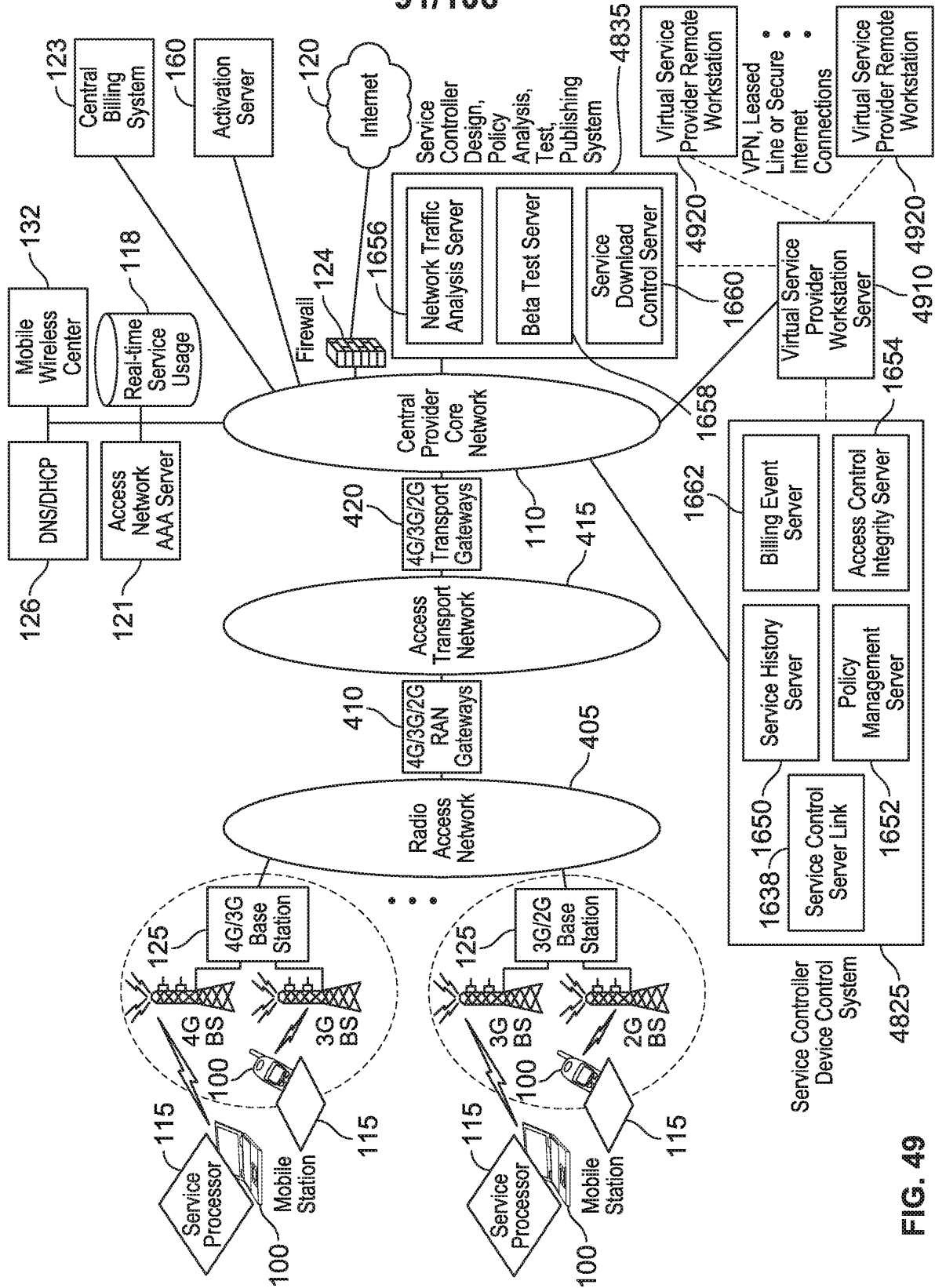


FIG. 49

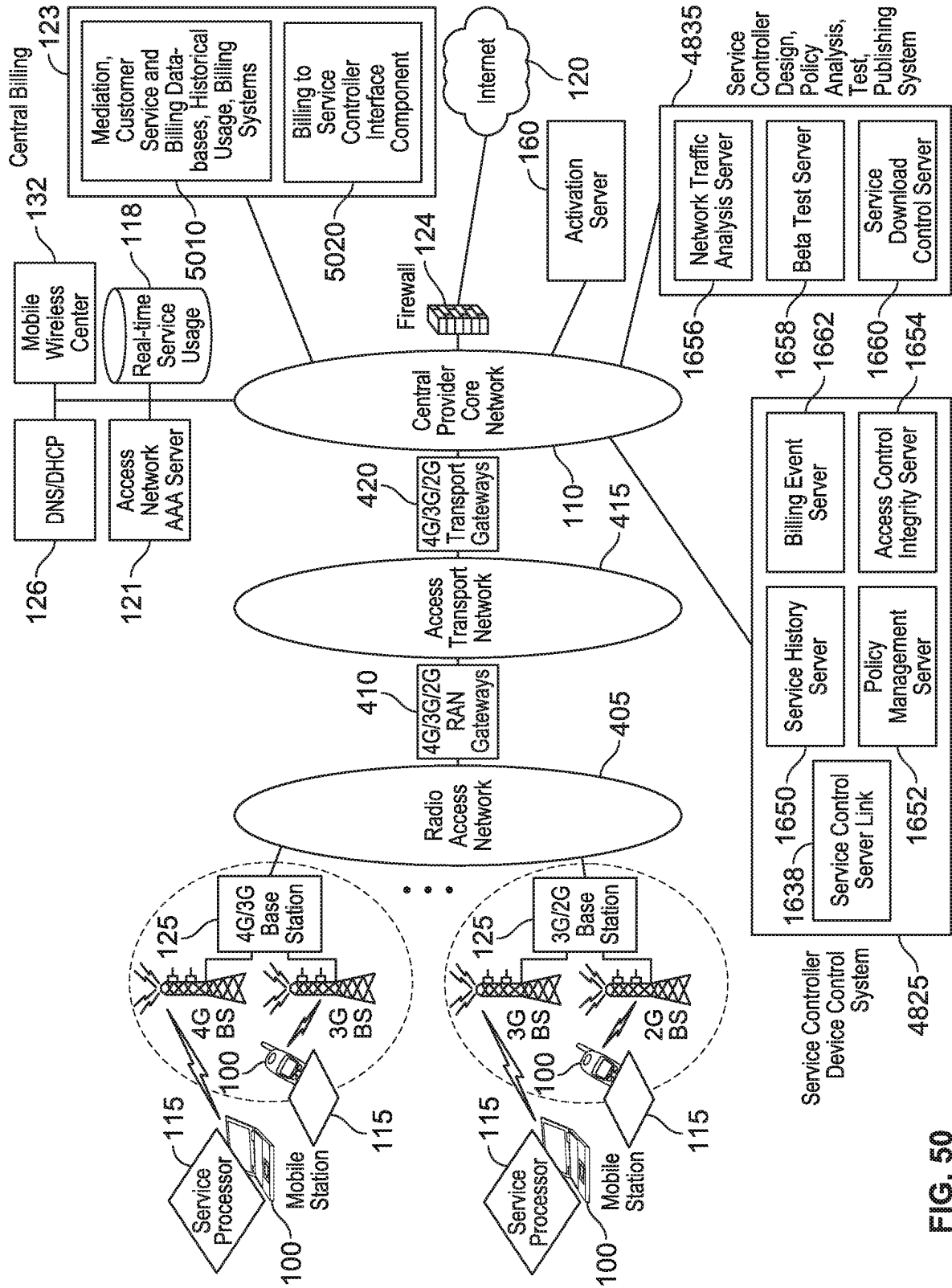


FIG. 50

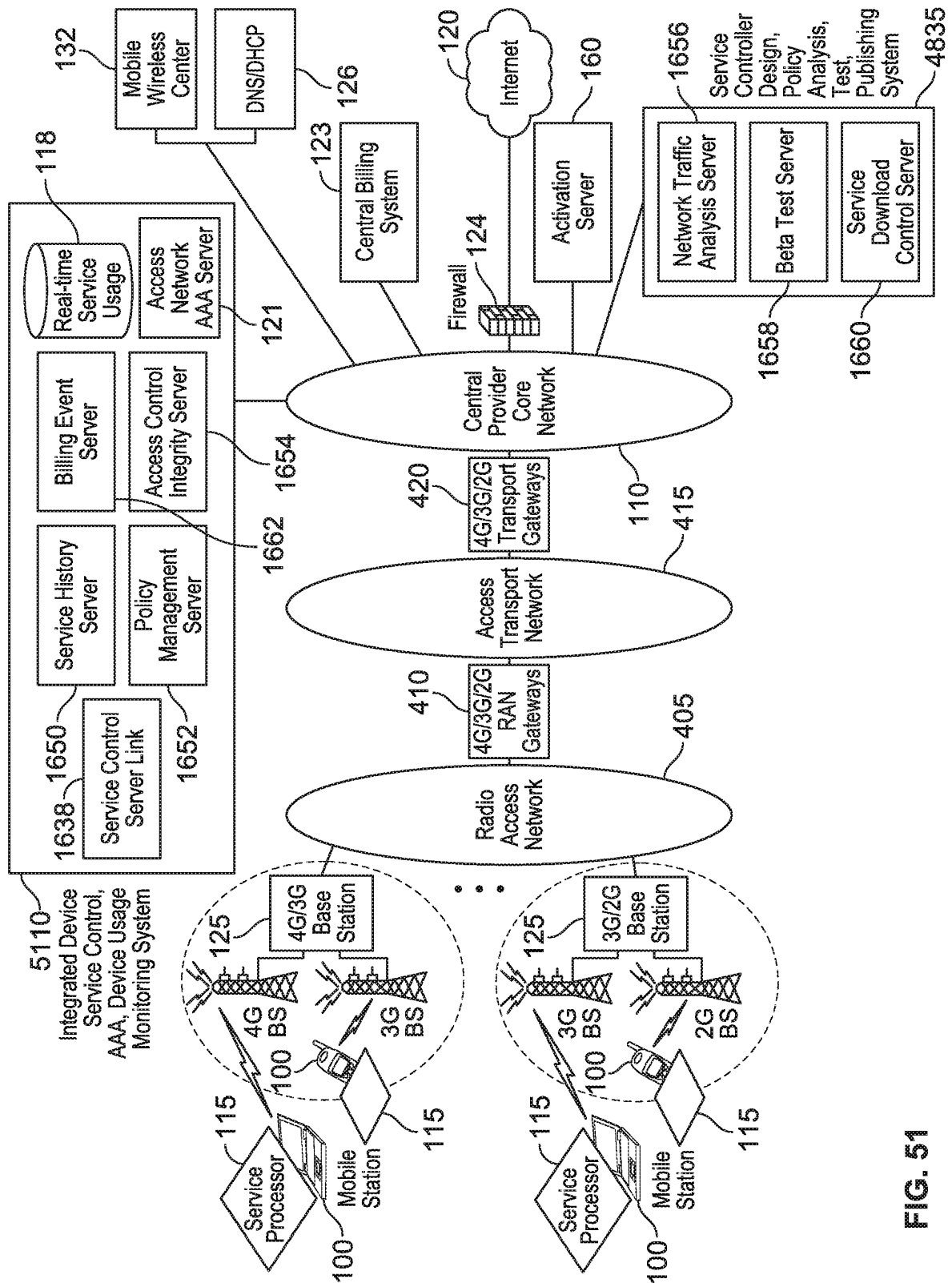


FIG. 51

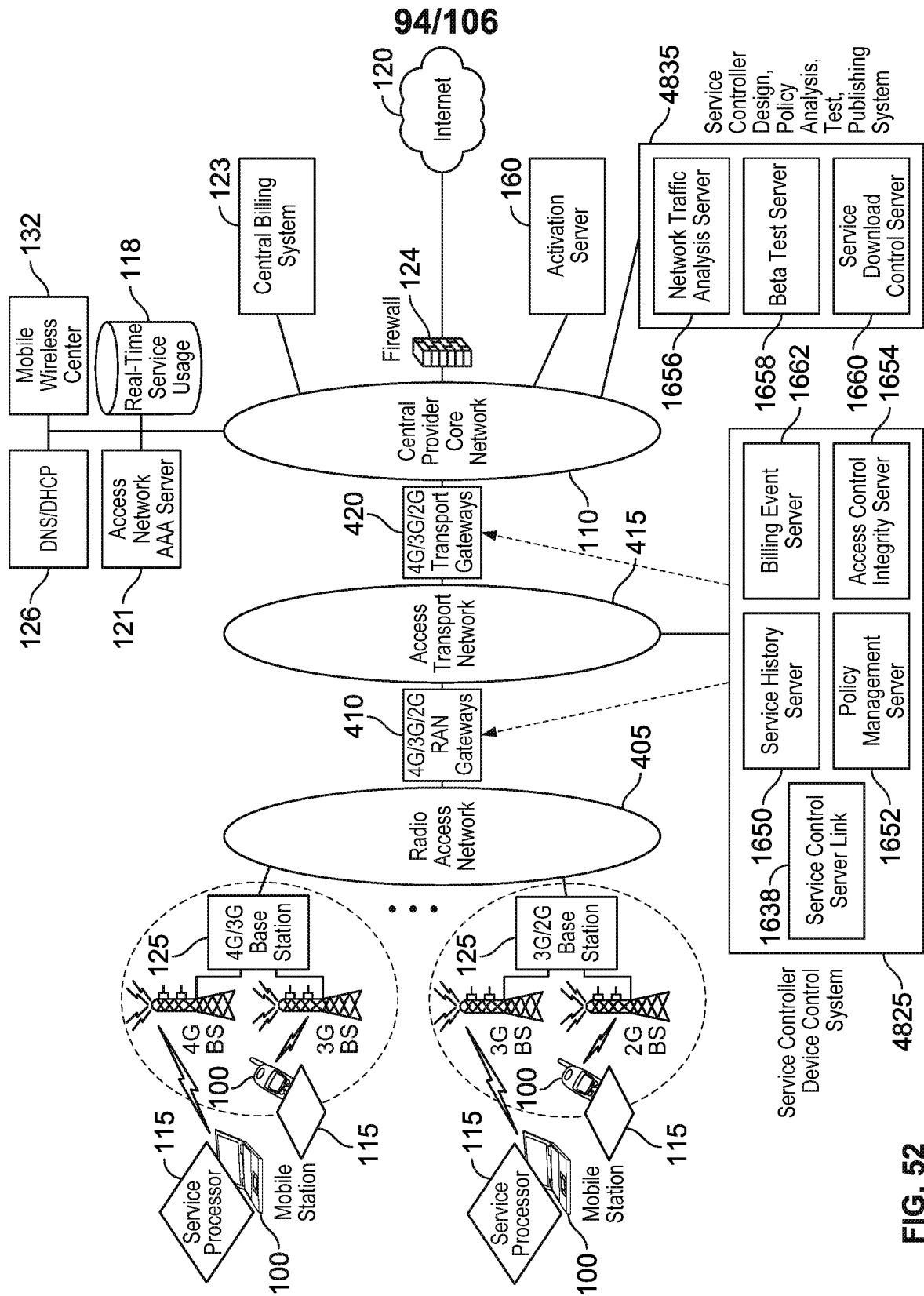


FIG. 52

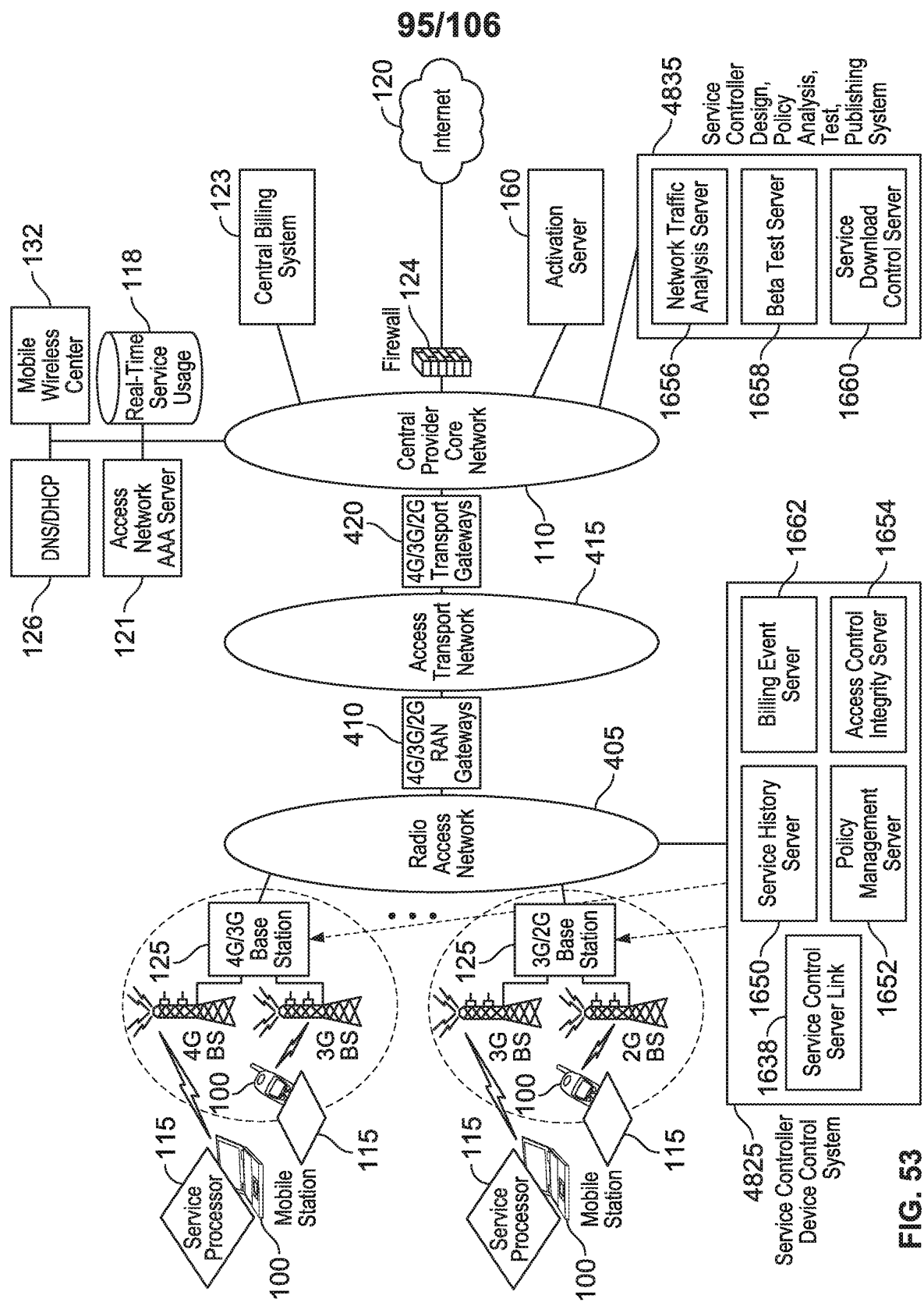


FIG. 53

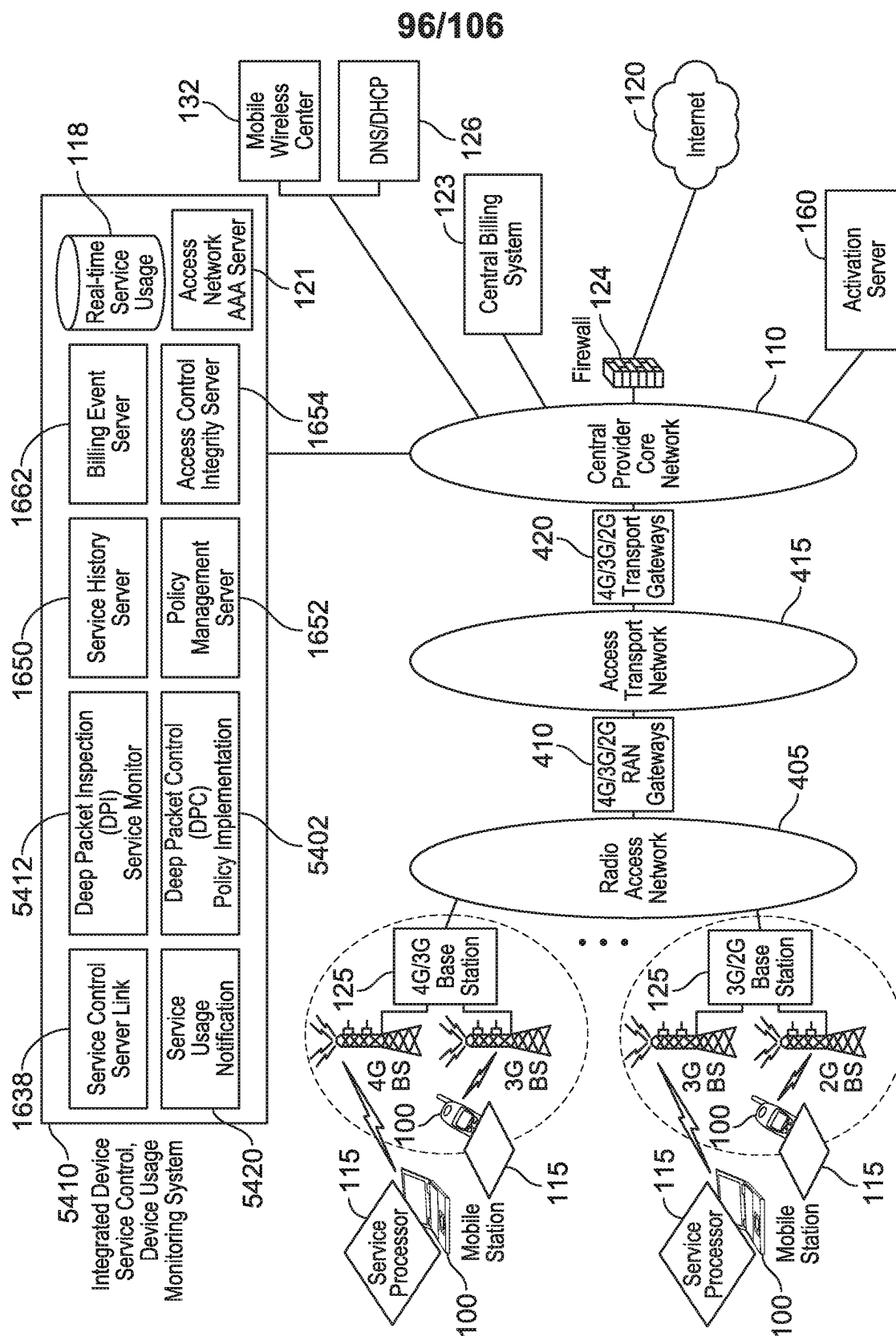


FIG. 54

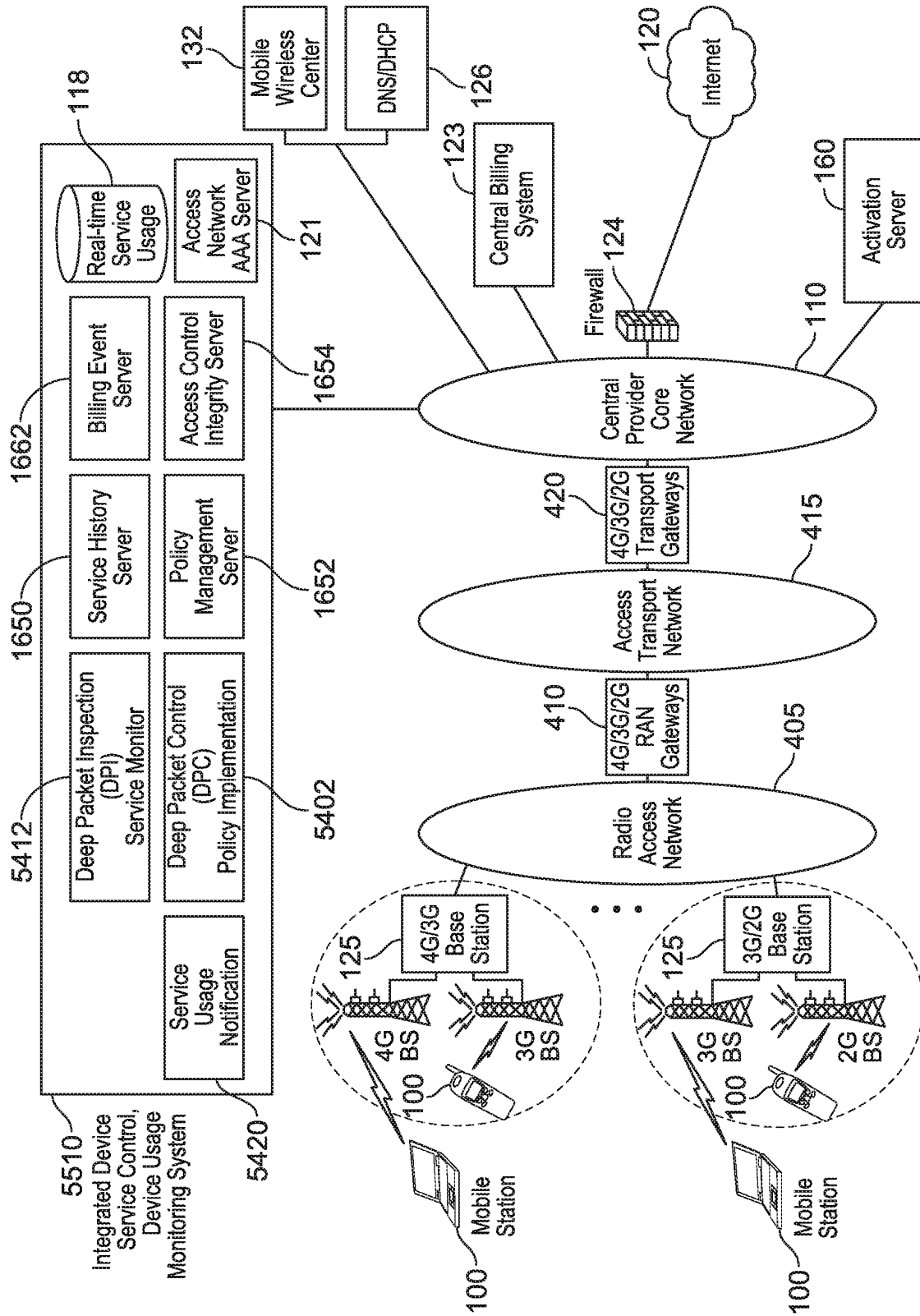


FIG. 55

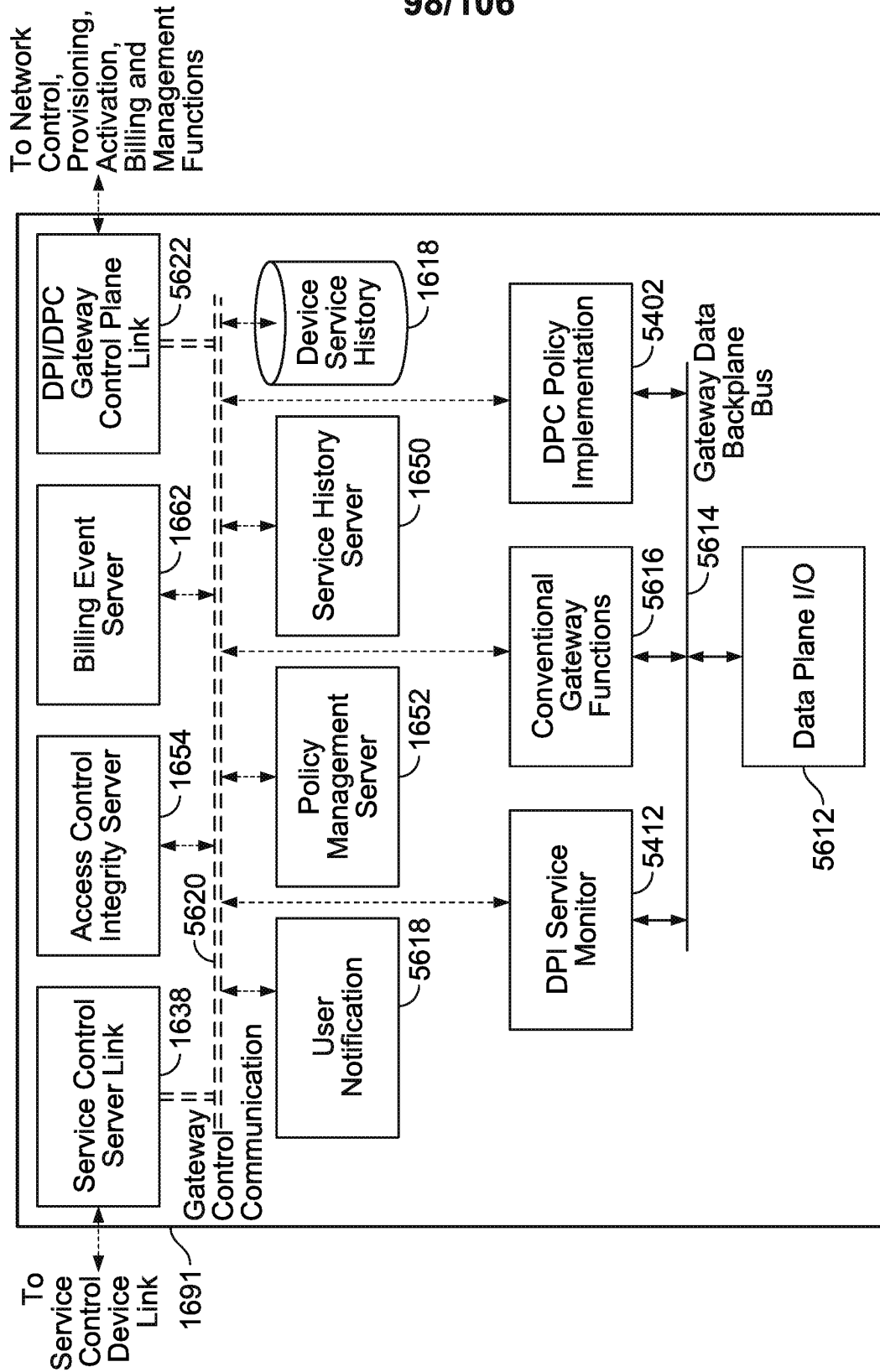


FIG. 56

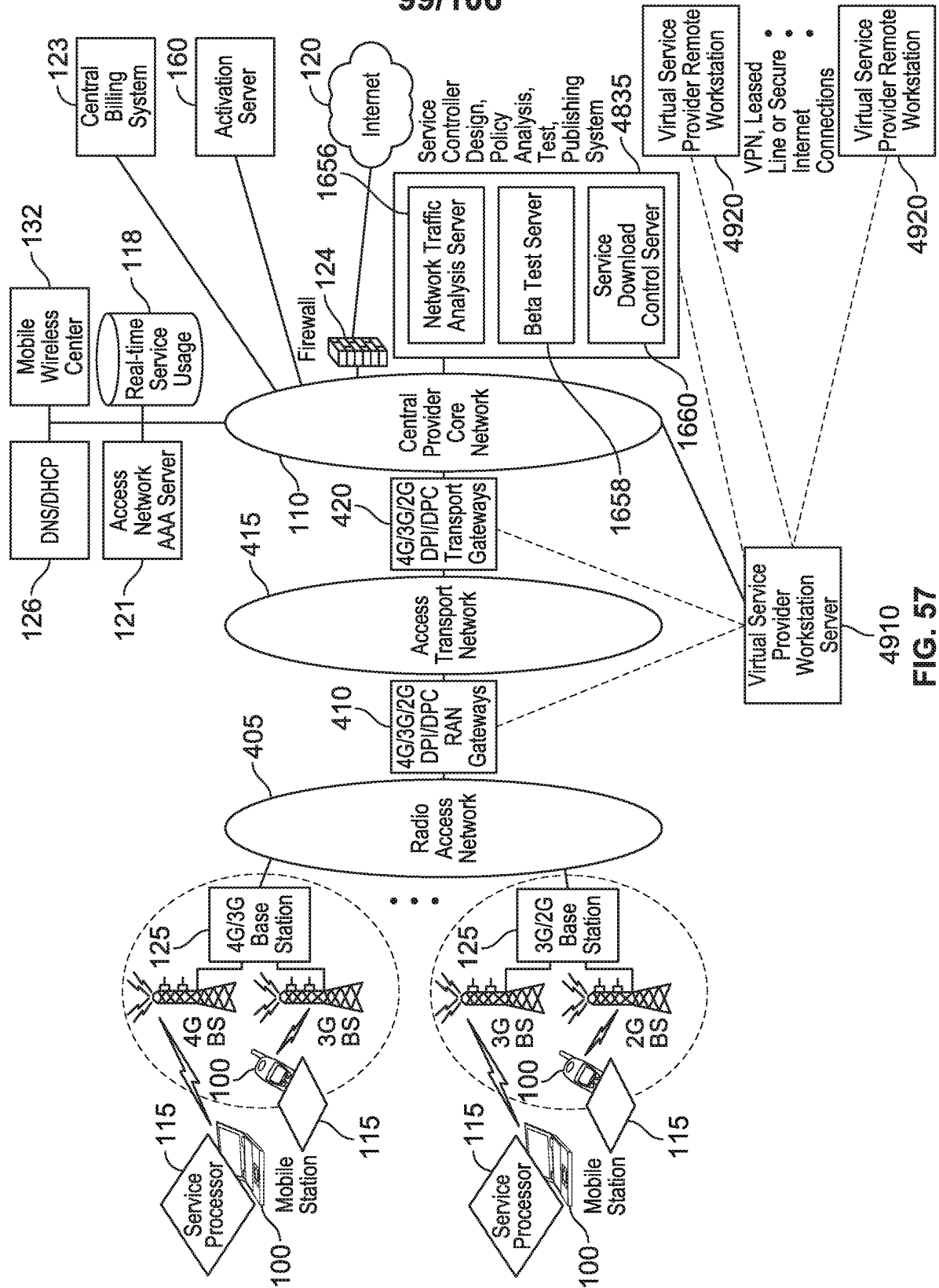


FIG. 57

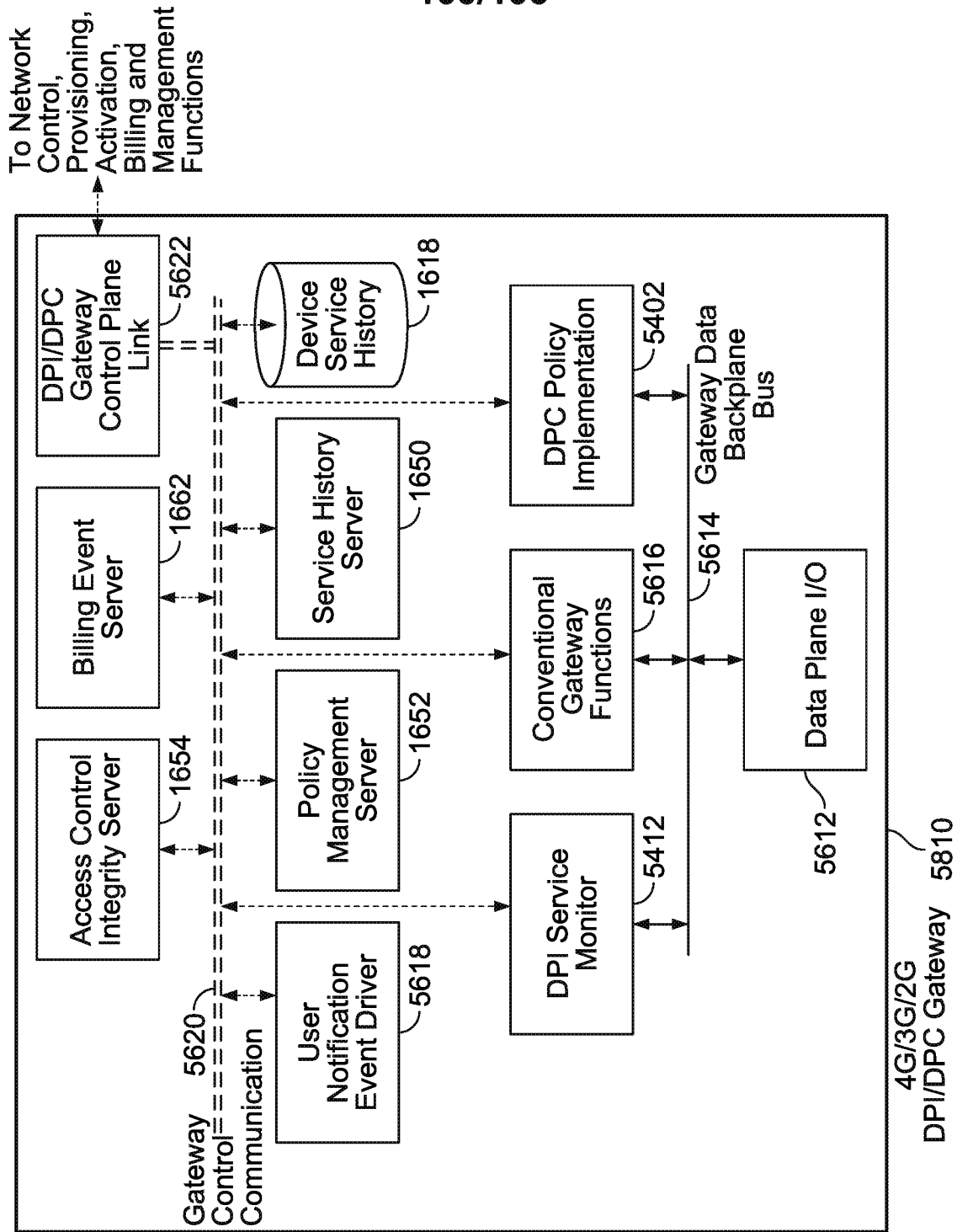


FIG. 58

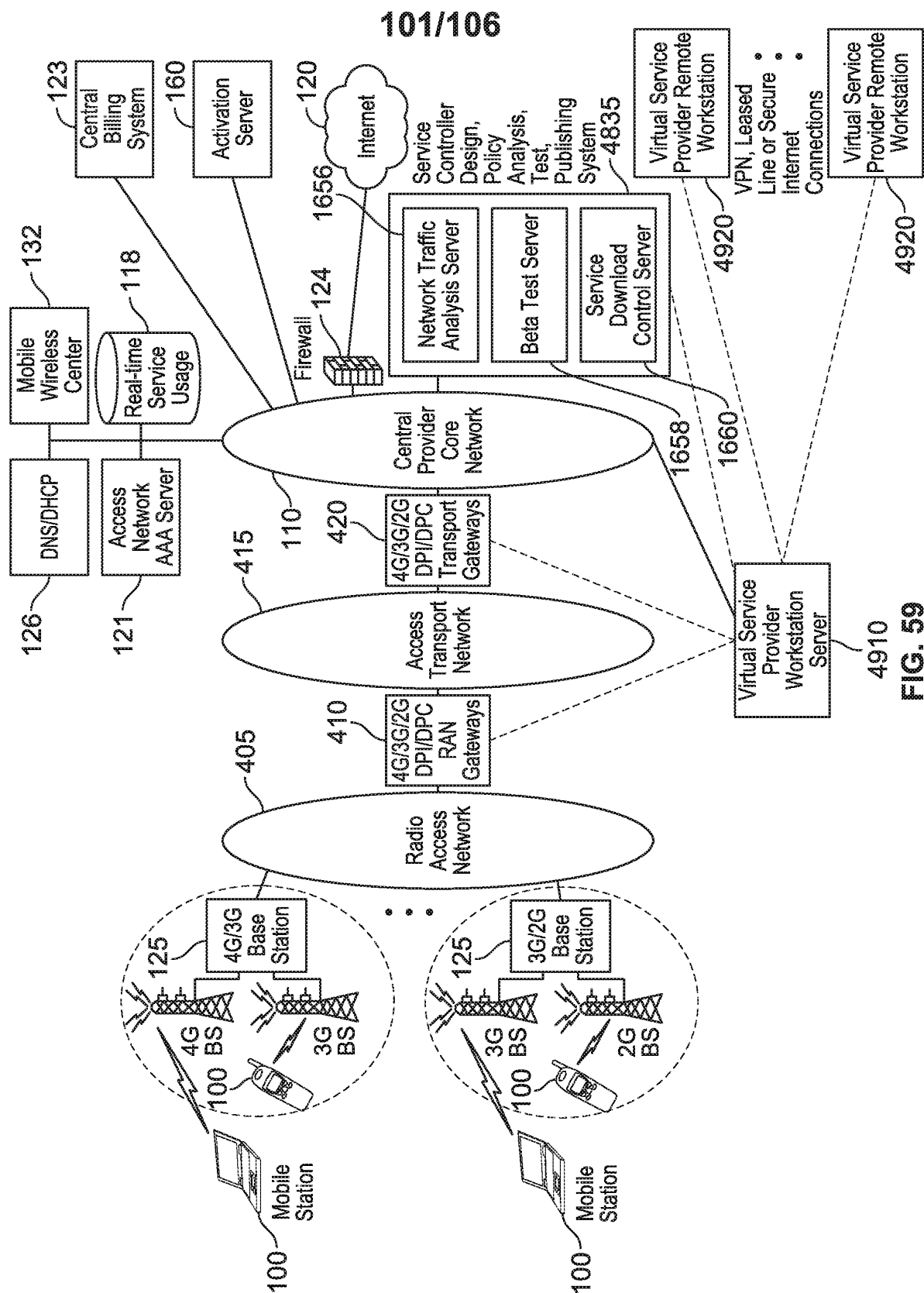
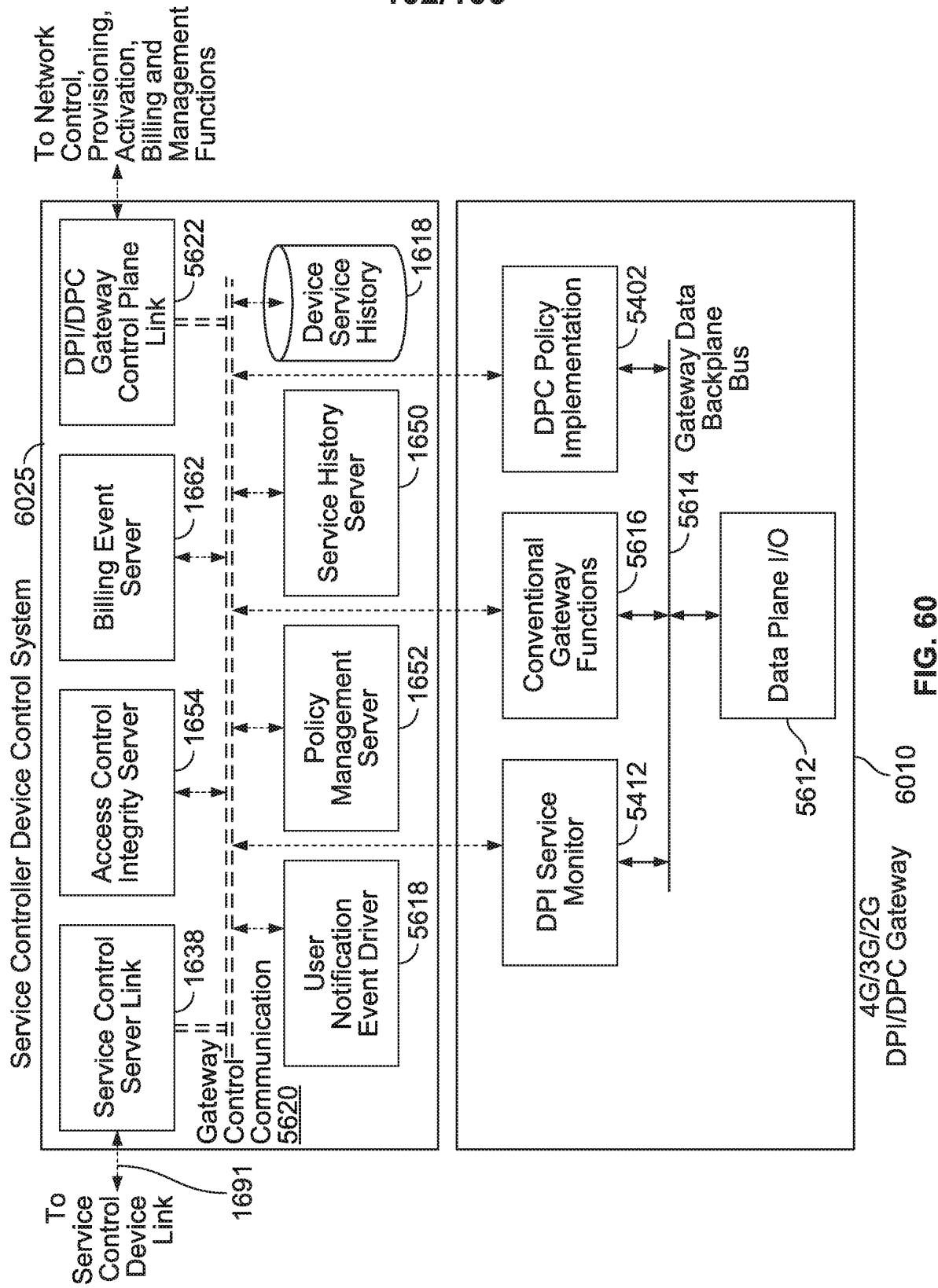


FIG. 59



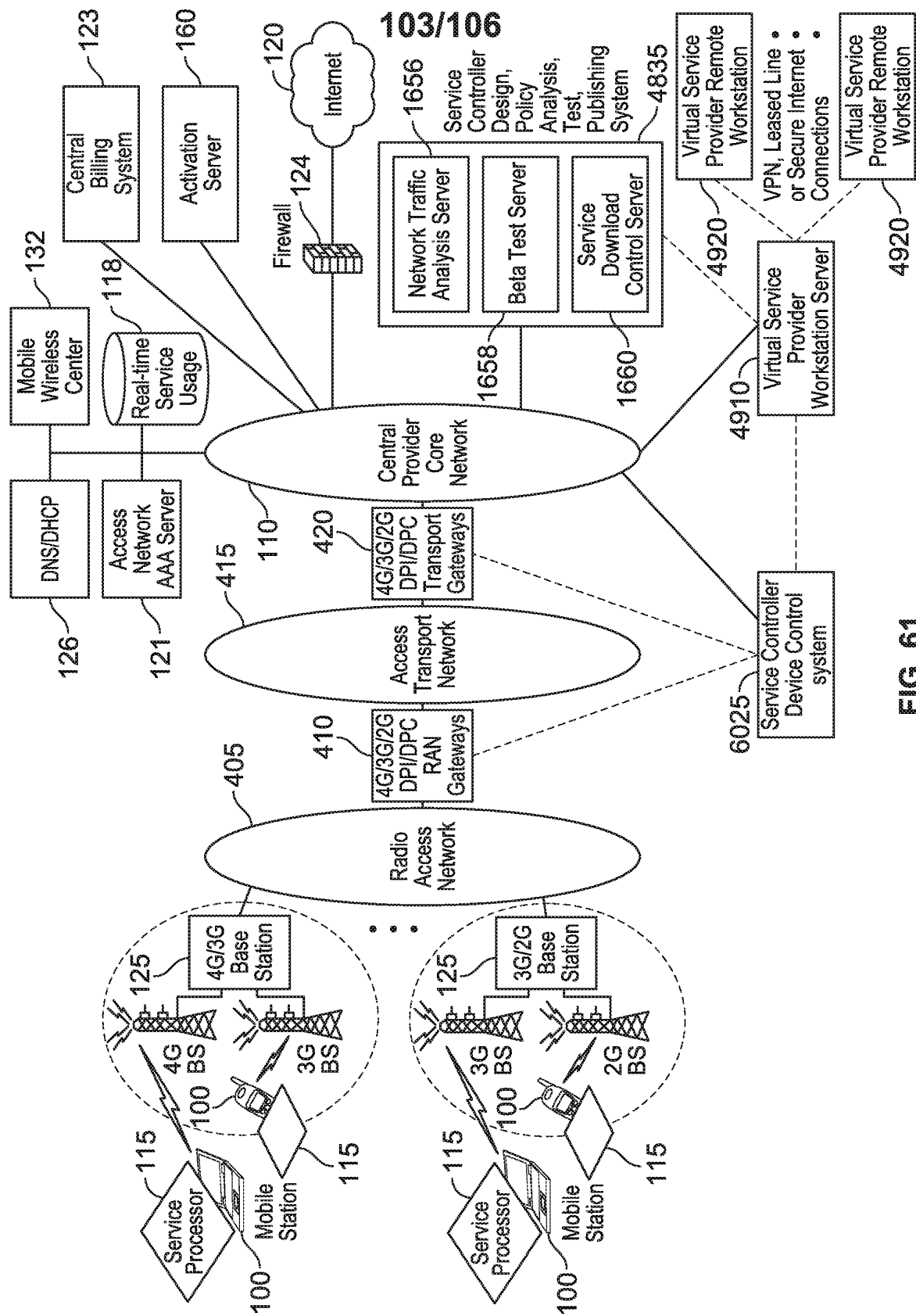
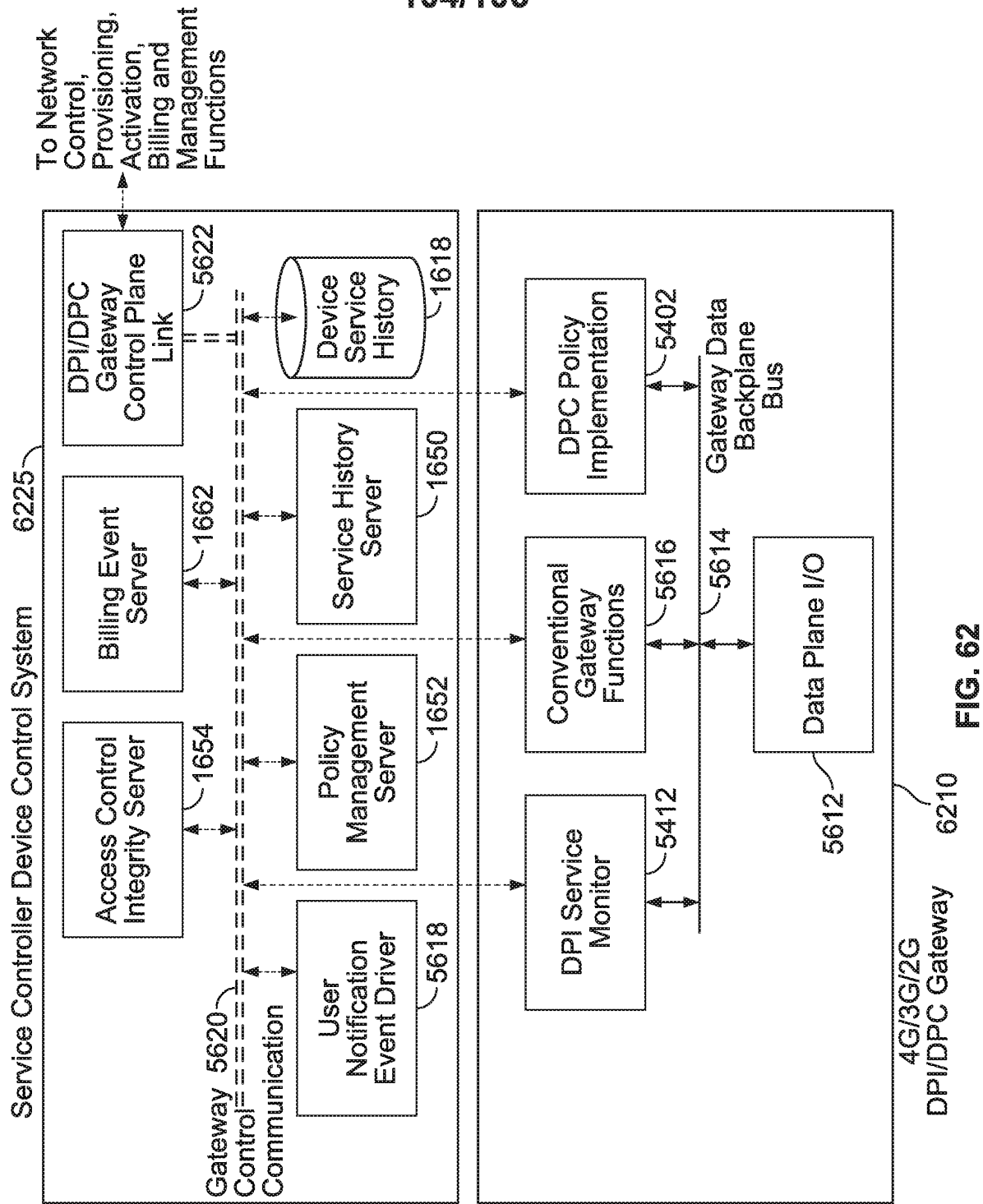


FIG. 61



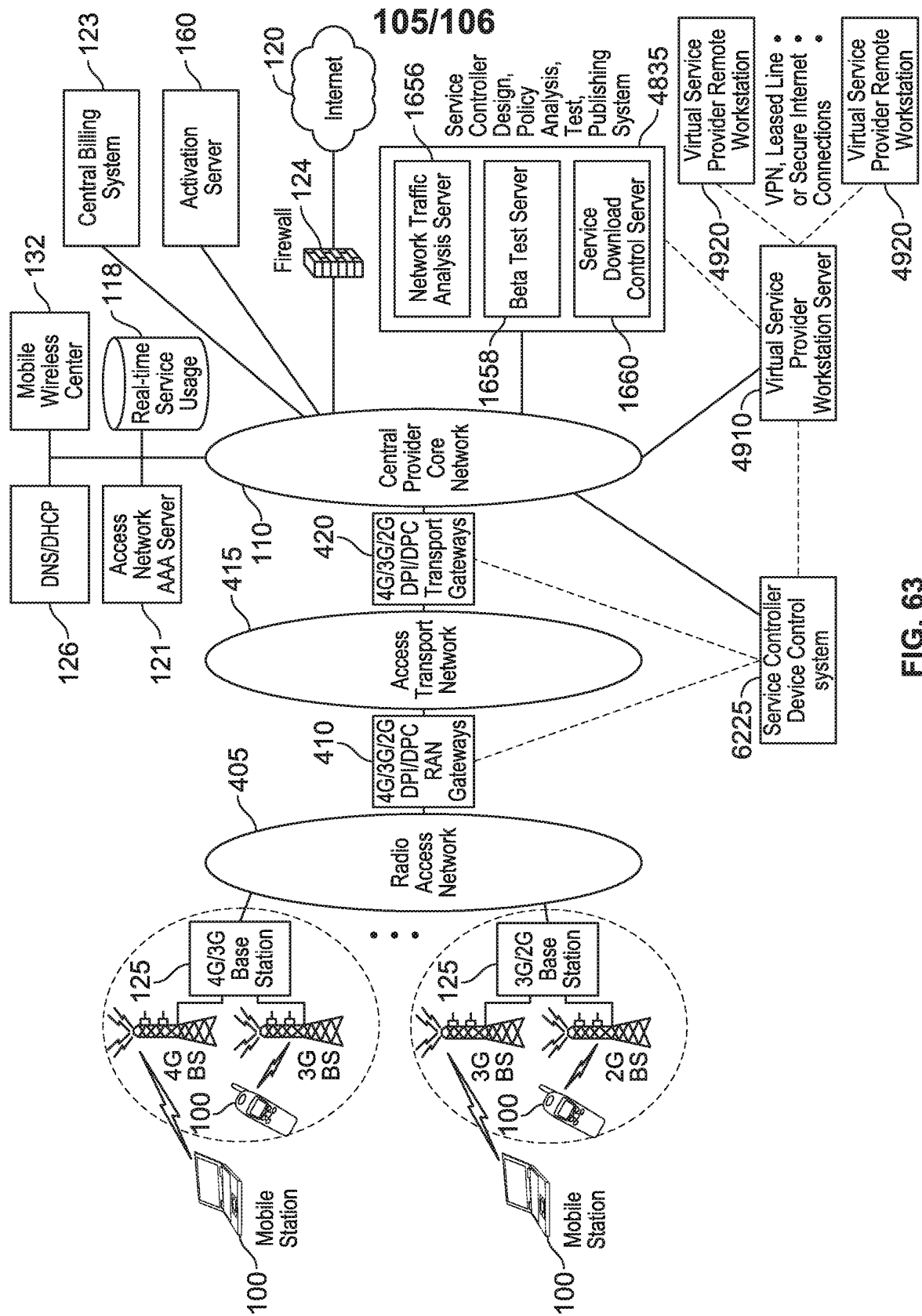


FIG. 63

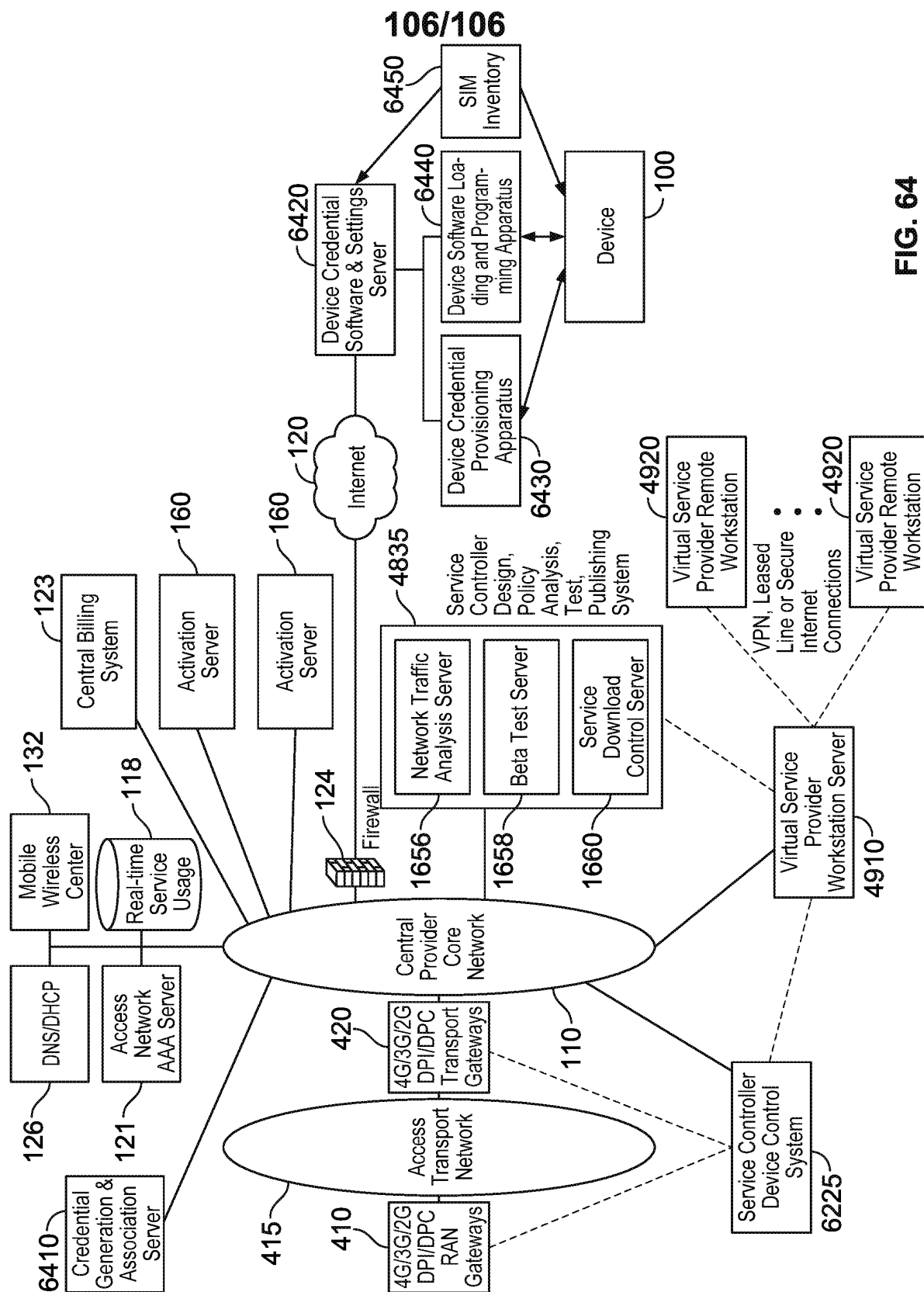


FIG. 64

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor	1 Remove				
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Gregory	G.	Raleigh		
Residence Information (Select One) • US Residency Non US Residency Active US Military Service					
City	Incline Village	State/Province	NV	Country of Residence	US
Mailing Address of Inventor:					
Address 1	110 N. College Avenue				
Address 2	Suite 1116				
City	Tyler	State/Province	TX		
Postal Code	75702	Country	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence information of this application.			
Customer Number	106963		
Email Address	patent@headwaterllc.com	Add Email	Remove Email

Application Information:

Title of the Invention	Automated Device Provisioning and Activation		
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	106	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	106963		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
this application	Continuation of	16436628	2019-06-10

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	
		Application Number			
Title of Invention		Automated Device Provisioning and Activation			

Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16436628	Continuation of	15582350	2017-04-28	10321320	2019-06-11
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15582350	Continuation of	15239398	2016-08-17	9641957	2017-05-02
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15239398	Continuation of	14979233	2015-12-22	9532161	2016-12-27
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14979233	Continuation of	14667353	2015-03-24	9232403	2016-01-05
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14667353	Continuation of	14263604	2014-04-28	9037127	2015-05-19
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14263604	Continuation of	12380780	2009-03-02	8839388	2014-09-16
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61206354	2009-01-28		
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61206944	2009-02-04		
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61207393	2009-02-10		
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61207739	2009-02-13		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant	1	<input type="button" value="Remove"/>	
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>			
		<input type="button" value="Clear"/>	
☐ Assignee	Legal Representative under 35 U.S.C. 117		Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>			
Name of the Deceased or Legally Incapacitated Inventor: <div style="border: 1px solid black; width: 400px; height: 20px;"></div>			
If the Applicant is an Organization check here. ☒			
Organization Name	Headwater Research LLC		
Mailing Address Information For Applicant:			
Address 1	110 N. College Avenue		
Address 2	Suite 1116		
City	Tyler	State/Province	TX
Country	US	Postal Code	75702
Phone Number	903-201-6212	Fax Number	
Email Address	patent@headwaterllc.com		
Additional Applicant Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Assignee 1			
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
			<input type="button" value="Remove"/>
If the Assignee or Non-Applicant Assignee is an Organization check here. ☒			
Organization Name	Headwater Research LLC		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	110 N. College Avenue		
Address 2	Suite 1116		
City	Tyler	State/Province	TX
Country i	US	Postal Code	75702
Phone Number	903-201-6212	Fax Number	
Email Address	patent@headwaterllc.com		
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a juristic entity (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, all joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of all joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/James E. Harris/		Date (YYYY-MM-DD)	2022-01-17	
First Name	James E.	Last Name	Harris	Registration Number	40013
Additional Signature may be generated within this form by selecting the Add button.				<input type="button" value="Add"/>	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

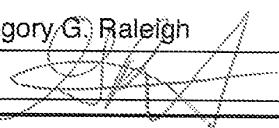
Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Gregory G. Raleigh</u> Date (Optional) : _____</p> <p>Signature: <u></u></p> <p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	44760065
Application Number:	17577237
International Application Number:	
Confirmation Number:	5850
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	GREGORY RALEIGH
Customer Number:	106963
Filer:	James E. Harris/Jennifer Smith
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3C2C3C2C1C1C1
Receipt Date:	17-JAN-2022
Filing Date:	
Time Stamp:	16:26:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Specification	final_spec.pdf	1088044	no	240
			b20c005fc37dc26a85cb08a06984c410d0cf4f50		

Warnings:

Information:					
2	Claims	CLAIMS.pdf	37070	no	1
			0da64783b669704fb29131c2bcd8b930605ccc6		
Warnings:					
Information:					
3	Abstract	abstract.pdf	38019	no	1
			400aab7ff5af812024b45f62fa42be5c00bfff62c		
Warnings:					
Information:					
4	Drawings-only black and white line drawings	Drawings.pdf	10157110	no	106
			a620d6d5a3712df05a679648f6b3c9d78a6d2c29		
Warnings:					
Information:					
5	Application Data Sheet	ADS.pdf	1823813	no	9
			cac0177f8f73de1d591555ea702eb78ed0c54ef3		
Warnings:					
Information:					
6	Oath or Declaration filed	Raleigh_Declaration.pdf	99297	no	1
			f767b71a3d35b8e258cd5b2b75cb8e48ce66a9b		
Warnings:					
Information:					
Total Files Size (in bytes):			13243353		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

106963 7590 08/21/2024
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

EXAMINER
MURILLO GARCIA, FABRICIO R

ART UNIT PAPER NUMBER
2633

DATE MAILED: 08/21/2024

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007/C11C3C2C3C2C1C1C1	5850

TITLE OF INVENTION: Automated Device Provisioning and Activation

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	11/21/2024

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via the USPTO patent electronic filing system.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 08/21/2024

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via the USPTO patent electronic filing system or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

17/577,237

01/17/2022

Gregory G. Raleigh

RALEP007C11C3C2C3C2C1C1C1

5850

TITLE OF INVENTION: Automated Device Provisioning and Activation

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	11/21/2024

EXAMINER	ART UNIT	CLASS-SUBCLASS
MURILLO GARCIA, FABRICIO R	2633	455-406000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required)

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via the USPTO patent electronic filing system ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850
106963	7590	08/21/2024	EXAMINER	
Headwater Research LLC C/O Farjami & Farjami LLP 26522 La Alameda Ave., Suite 360 Mission Viejo, CA 92691			MURILLO GARCIA, FABRICIO R	
			ART UNIT	PAPER NUMBER
			2633	
DATE MAILED: 08/21/2024				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.** Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013).

<https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to:

- 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law;
- 2) a federal, state, local, or international agency, in response to its request;
- 3) a contractor of the USPTO having need for the information in order to perform a contract;
- 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record;
- 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record;
- 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations;
- 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals;
- 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c));
- 9) the Office of Personnel Management (OPM) for personnel research purposes; and
- 10) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Notice of Allowability	Application No. 17/577,237	Applicant(s) Raleigh, Gregory G.	
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 07/29/2024.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 2-16. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)	5. ☒ Examiner's Amendment/Comment
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.	6. ☒ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____.	

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **29 July 2024** has been entered.

Response to Arguments

Following response to arguments is based on Applicant's arguments filed on **18 July 2024**.

Regarding Previous Claim Objections

Previous objection to claims **2, 4, 7, 9, 12, 14** has been withdrawn in view of the amendments to the objected claims.

Regarding Previous Rejection Under 35 USC § 112

Previous rejection of claims **2-16** has been withdrawn in view of the amendment

to the rejected claims.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for the following examiner's amendment was given in a telephone interview with **Farshad Farjami (Reg. No. 41,014) on 07 August 2024.**

In the claims, the Examiner's Amendment is as follows:

Claims **2, 7, 12** have been amended as follows:

Claim 2 (Currently Amended): A network message server adapted to communicate with a mobile end-user device having a plurality of applications, the network message server comprising:

one or more processors configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the received request corresponding to a first application of the plurality of **applications**;

generate an Internet data message based on the received request, the

generated Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and **for** forwarding the application data in the transmitted Internet data message to the first application mapped by the mobile end-user device to the first application identifier.

Claim 7 (Currently Amended): A method for use by a network message server adapted to communicate with a mobile end-user device having a plurality of applications, the method comprising:

providing a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receiving a request to transmit application data, the received request corresponding to a first application of the plurality of **applications**;

generating an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and

transmitting, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and **for** forwarding the application data in the

transmitted Internet data message to the first application mapped by the mobile end-user device to the first application identifier.

Claim 12 (Currently Amended): A network system comprising:

- a mobile end-user device having a plurality of applications;
- a network message server adapted to communicate with the mobile end-user device, the network message server configured to:
 - provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;
 - receive a request to transmit application data, the received request corresponding to a first application of the plurality of **applications**;
 - generate an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and
 - transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device;
- the mobile end-user device configured to:
 - receive the transmitted Internet data message from the network message server;
 - map the first application identifier included in the received Internet data message to the first application corresponding to the first application identifier; and
 - forward the application data in the received Internet data message to the first application mapped by the mobile end-user device to the first application identifier.

Allowable Subject Matter

Claims **2-16** are allowed.

The following is an examiner's statement of reasons for allowance:

Regarding claim 2, the prior art of record does not show or suggest the combination of the following limitations: “*transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and forward the application data in the transmitted Internet data message to the first application mapped by the mobile end-user device to the first application identifier*”.

Regarding claims 7 and 12, these claims are also allowed as they incorporate limitations similar to those set forth in independent claim 2.

It is the claim, taken as a whole, including the interrelationships and interconnections between the various claimed elements, that which make it allowable over the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Alharayeri US Patent Application Publication No. 2016/0135014 teaches location-based discovery of network members by personal attributes using dynamic and static location data.
2. Newell US Patent Application Publication No. 2009/0328197 teaches user validation using images.
3. Shima et al. US Patent Application Publication No. 2016/0105438 teaches system, method, and apparatus for authentication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FABRICIO R MURILLO GARCIA whose telephone number is (571)270-5708. The examiner can normally be reached 9-5pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sam K Ahn can be reached on 5712723044. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

August 10, 2024

/FABRICIO R MURILLO GARCIA/
Primary Examiner, Art Unit 2633

<i>Examiner-Initiated Interview Summary</i>	Application No. 17/577,237	Applicant(s) Raleigh, Gregory G.		
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633	AIA (First Inventor to File) Status No	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
FABRICIO R MURILLO GARCIA	Primary Examiner	Telephonic
Farshad Farjami (Reg. No. 41,014)	Attorney of Record	

Date of Interview: 07 August 2024

Issues Discussed:

Other

Discussed about amending independent claims 2, 7 and 12, by correcting minor issues, thus placing the application in condition for allowance. Agreement was reached. Details of the agreement are in the Notice of Allowability

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
<p>Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04</p> <p>Please further see: MPEP 713.04 Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b) 37 CFR § 1.2 Business to be transacted in writing</p>	

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Notice of References Cited	Application/Control No. 17/577,237		Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.	
	Examiner FABRICIO R MURILLO GARCIA		Art Unit 2633	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20160135014-A1	2016-05-12	Alharayeri; Ramzi	H04L67/306	455/456.3
*	B	US-20090328197-A1	2009-12-31	Newell; Mark Dwight	G06F21/36	345/168
*	C	US-20160105438-A1	2016-04-14	SHIMA; Taira	H04L63/0884	726/4
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC - Searched*		
Symbol	Date	Examiner
G06F15/177	03/09/2024	FM
H04W28/0215	03/09/2024	FM

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
455/406		03/09/2024	FM

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

Search Notes		
Search Notes	Date	Examiner
East (See Attachment)	03/09/2024	FM
Inventor Search (search for double patenting)	03/09/2024	FM
Non Patentable Literature	03/09/2024	FM
455/406 - See Attached East Search	03/09/2024	FM
G06F15/177 - See Attached East Search	03/09/2024	FM
H04W28/0215 - See Attached East Search	03/09/2024	FM
Updated	06/25/2024	FM
Updated	08/06/2024	FM
455/406 Interference Search - See Attached East Search	08/06/2024	FM
G06F15/177 Interference Search - See Attached East Search	08/06/2024	FM
H04W28/0215 Interference Search - See Attached East Search	08/06/2024	FM

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
455/406		08/06/2024	FM
G06F15/177		08/06/2024	FM
H04W28/0215		08/06/2024	FM

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC						
Symbol					Type	Version
H04L	/	63	/	20	F	2013-01-01
G06Q	/	10	/	06375	I	2013-01-01
G06Q	/	20	/	102	I	2013-01-01
G06Q	/	20	/	20	I	2013-01-01
G06Q	/	20	/	40	I	2013-01-01
G06Q	/	30	/	0207	I	2013-01-01
G06Q	/	30	/	0283	I	2013-01-01
G06Q	/	30	/	0284	I	2013-01-01
G06Q	/	30	/	04	I	2013-01-01
G06Q	/	30	/	0601	I	2013-01-01
G06Q	/	40	/	00	I	2013-01-01
H04L	/	12	/	14	I	2013-01-01
H04L	/	41	/	0893	I	2013-01-01
H04M	/	15	/	00	I	2013-01-01
H04M	/	15	/	58	I	2013-01-01
H04W	/	88	/	08	I	2013-01-01
H04L	/	63	/	0236	I	2013-01-01
H04L	/	67	/	306	I	2013-01-01
G06Q	/	40	/	12	I	2013-01-01
H04W	/	4	/	50	I	2018-02-01
H04W	/	12	/	037	I	2021-01-01
H04L	/	67	/	55	I	2022-05-01
H04L	/	67	/	63	I	2022-05-01
H04L	/	41	/	5003	I	2013-01-01
H04W	/	4	/	24	I	2013-01-01
G06F	/	15	/	177	I	2013-01-01
G06Q	/	30	/	0241	I	2013-01-01
H04L	/	9	/	32	I	2013-01-01
H04L	/	63	/	10	I	2013-01-01
H04W	/	28	/	02	I	2013-01-01
H04W	/	12	/	08	I	2013-01-01

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	06 August 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	2	3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC						
Symbol				Type	Version	
H04L	/	47	/	2408	I	2013-01-01
H04L	/	63	/	08	I	2013-01-01
H04W	/	8	/	20	I	2013-01-01
H04W	/	28	/	12	I	2013-01-01
H04W	/	48	/	14	I	2013-01-01
H04W	/	4	/	20	I	2013-01-01
H04W	/	12	/	00	I	2013-01-01
H04M	/	15	/	88	I	2013-01-01
H04W	/	28	/	0268	I	2013-01-01
H04M	/	15	/	61	I	2013-01-01
H04W	/	24	/	08	I	2013-01-01
H04W	/	12	/	02	I	2013-01-01
H04L	/	51	/	046	I	2013-01-01
H04L	/	63	/	0428	I	2013-01-01
H04W	/	4	/	12	I	2013-01-01
H04W	/	4	/	18	I	2013-01-01
H04W	/	8	/	18	I	2013-01-01
H04W	/	72	/	0453	I	2013-01-01
H04L	/	47	/	20	I	2013-01-01
H04W	/	28	/	0215	I	2013-01-01
H04W	/	4	/	02	I	2013-01-01
G06Q	/	10	/	06315	I	2013-01-01
H04L	/	41	/	0806	I	2013-01-01
H04L	/	41	/	5054	I	2013-01-01
H04M	/	15	/	80	I	2013-01-01
H04L	/	63	/	04	I	2013-01-01
H04L	/	9	/	3247	I	2013-01-01
H04L	/	63	/	0892	I	2013-01-01
H04L	/	67	/	145	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
H04L	/	63	/	0853	I	2013-01-01

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	06 August 2024	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	2	3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC						
Symbol					Type	Version
H04W	/	48	/	16	I	2013-01-01
H04L	/	41	/	5025	A	2013-01-01
H04M	/	2215	/	0188	A	2013-01-01
H04L	/	67	/	34	A	2013-01-01
H04W	/	8	/	02	A	2013-01-01
Y02P	/	90	/	80	A	2015-11-01
H04L	/	67	/	564	A	2022-05-01
H04W	/	84	/	04	A	2013-01-01
H04W	/	84	/	12	A	2013-01-01
H04W	/	88	/	06	A	2013-01-01
H04W	/	84	/	042	A	2013-01-01
H04L	/	41	/	0876	A	2013-01-01

CPC Combination Sets					
Symbol				Type	Set
	/		/		

NONE (Assistant Examiner)		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner)		06 August 2024 (Date)	
		O.G. Print Claim(s) 2	O.G. Print Figure 3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04L9/40	/	9	40
G06Q10/0637	/	10	0637
G06Q20/10	/	20	10
G06Q20/20	/	20	20
G06Q20/40	/	20	40
G06Q30/0207	/	30	0207
G06Q30/0283	/	30	0283
G06Q30/04	/	30	04
G06Q30/0601	/	30	0601
G06Q40/00	/	40	00
H04L12/14	/	12	14
H04L41/0893	/	41	0893
H04M15/00	/	15	00
H04W88/08	/	88	08
H04L67/306	/	67	306
G06Q40/12	/	40	12
H04W4/50	/	4	50
H04W12/037	/	12	037
H04L67/55	/	67	55
H04L67/63	/	67	63
NON-CLAIMED			
	/		

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
455	406

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 2	O.G. Print Figure 3

<i>Issue Classification</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE (Assistant Examiner) (Date)		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner)		06 August 2024 (Date)	
		O.G. Print Claim(s) 2	O.G. Print Figure 3

Issue Classification 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
-	1		10												
	2		11												
	3		12												
	4		13												
	5		14												
	6		15												
	7		16												
	8														
	9														

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 15	
/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633 (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 2	O.G. Print Figure 3

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	1	"17577237"	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:06 AM
L2	633	((("RALEIGH") near3 ("Gregory"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/03/09 06:10 AM
L3	1	((US-20220279021-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:19 PM
L4	3098	(store) WITH ((device) near2 (credential))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:36 PM
L5	2	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L6	0	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal) WITH (activate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L7	30	("6178511" "6243816" "7249182" "7296036" "7310515" "7346855" "7353462" "8472874" "8606854" "20040009750" "20040113807" "20050026594" "20050076124" "20050193093" "20050281237" "20060063548" "20060234631" "20070021111" "20070167136" "20070168425" "20070242814" "20070260751" "20080051033" "20080108308" "20090209202").pn. OR ("9357352").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:38 PM
L8	4	((US-11304026-B2 OR US-10963844-B2 OR US-10250549-B2 OR US-9609673-B2).did. AND USPT.dbnm.)	(USPAT)	OR	ON	ON	2024/03/09 06:38 PM
L9	4	((US-8606854-B2 OR US-8472874-B2).did.	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM

L10	4	AND USPT.dbnm.) OR ((US-20090209202-A1 OR US-20080108308- A1).did. AND PGPB.dbnm.) ((US-7353462-B2 OR US-7346855-B2 OR US-7296036-B2).did. AND USPT.dbnm.) OR ((US-20080051033- A1).did. AND PGPB.dbnm.)	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L11	4	((US-20070260751-A1 OR US-20070242814- A1 OR US- 20070167136-A1 OR US-20070168425- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L12	4	((US-20070021111-A1 OR US-20060234631- A1 OR US- 20060063548-A1 OR US-20050281237- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L13	41	("6867733" "7418268" "7686217" "7847684" "8010131" "8108414" "8655385" "8688143" "8892130" "9173245" "9203857" "9226105" "9268920" "9357352" "9485211" "9830562" "9940402" "10013489" "10049400" "10075822" "10078696" "10264609" "10575138" "10599390" "20040116106" "20100313142" "20130316735" "20130331087" "20140162698" "20150058427" "20150080027" "20150088672" "20150365787" "20150378587" "20160261985" "20160334545" "20160364811" "20180176166"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:39 PM

L14	2	"20190014220" "20190215660" "20210173880").pn. OR ("11304026").urpn. AND (PGPB USPT USOC).dbnm. (storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L15	5	(stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L16	5	(save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L17	5	(saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L18	5	(saved saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L19	6	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L20	30	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L21	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L22	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM

L23	72	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L24	75	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L25	759	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L26	762	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L27	128	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L28	88	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L29	78	(user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L30	66	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L31	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L32	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activae)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L33	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L34	1	(user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L35	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L36	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start begin)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:44 PM
L37	1	("2022/0124167").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:45 PM
L38	2	((US-20220279021-A1 OR US-20160135014- A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/03/09 06:45 PM
L39	1	(saved saving save stored storing store) near10 ((device sensor)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L40	1	near2 (credential) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L41	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L42	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began began begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L43	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L44	1	near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L45	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L46	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L47	4	starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) WITH ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L48	3	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L49	4	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L50	15	(saved saving save	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09

		stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) WITH (initiated initiating running starting run activate initiate start started began begun begin beginning)					06:56 PM
L51	4	((US-20220124167-A1 OR US-20200275225- A1 OR US- 20170006034-A1).did. AND PGPB.dbnm.) OR ((US-9554061-B1).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:59 PM
L52	3	((US-20140373012-A1 OR US-20140337940- A1 OR US- 20130191885-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:59 PM
L53	24	("6757837" "6882712" "6889510" "7355730" "20020082924" "20060236325" "20070225828" "20080167127" "20080167128" "20080167133" "20090078760" "20100112997" "20100268401" "20110113087" "20110202798" "20110294466" "20120129492" "20120221893" "20120226619" "20120324067" "20140028449" "20140173059").pn. OR ("9129127").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM
L54	88	("6564056" "7664707" "7908401" "8311513" "8447696" "8974544" "9129127" "9141150" "9183380" "9204298" "9246921" "9489250"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM

		"9507950" "9524174" "9531559" "9575477" "20040125782" "20050246243" "20080062258" "20080204199" "20090023395" "20100031371" "20100094981" "20110145927" "20130067551" "20130171981" "20130191885" "20130254437" "20130304795" "20130311684" "20140040989" "20140098247" "20140245765" "20140263612" "20140266669" "20140266679" "20140277597" "20140279109" "20140282486" "20140304632" "20140313048" "20140344454" "20140359042" "20140376528" "20150006686" "20150033305" "20150038129" "20150040246" "20150052578" "20150061859" "20150081928" "20150097689" "20150100618" "20150109104" "20150160935" "20150163412" "20150177705" "20150198938" "20150215337" "20150222578" "20150261954" "20150279134" "20150304171" "20150309548" "20150324179" "20150364028" "20160014108" "20160063854" "20160098362" "20160099972" "20160103494" "20160109864"				
--	--	--	--	--	--	--

		"20160119742" "20160142258" "20160142532" "20160294602" "20160337945" "20160351036" "20160380987" "20170019264" "20170034156" "20170034158" "20170046173" "20170048712" "20170078298" "20170093860" "20170099560" "20170109998").pn. OR ("10157271").urpn. AND (PGPB USPT USOC).dbnm.					
L55	4	((US-20170109998-A1 OR US-20170099560- A1 OR US- 20170093860-A1).did. AND PGPB.dbnm.) OR ((US-9575477-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:00 PM
L56	1	((US-20160135014- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 07:37 PM
L57	1	"8839388".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:49 PM
L58	1	"9037127".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:54 PM
L59	1	"9232403".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:56 PM
L60	1	"9532161".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:57 PM
L61	1	"9641957".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:58 PM
L62	1	"10321320".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:59 PM
L63	1	"11228617".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 08:00 PM
L64	8	"20090292815"	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 08:06 PM
L65	1	((US-20090292815- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 09:27 PM
L66	806072	(memory WITH instructions) AND ;65	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 09:27 PM
L67	0	(memory WITH instructions) AND L65	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 09:27 PM
L68	1	(memory SAME	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09

L69	2126	instructions) AND L65 ((secure) near2(internet)) WITH (application)	(US-PGPUB; USPAT)	OR	ON	ON	09:28 PM 2024/06/25 03:05 AM
L70	7	((secure) near2(internet)) WITH (application) WITH (communication ADJ device)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L71	8	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L72	14	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L73	56	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:08 AM
L74	78	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L75	90	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L76	90	((secure) near2(internet)) WITH (application) WITH	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM

L77	103	((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld cellphone))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L78	103	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld cellphone smartphone))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L79	103	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L80	144	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM

L81	3	terminal) (mobile ADJ device)) ((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L82	12	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L83	16	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L84	16	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM

L85	16	cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying) ((secure) near2(internet)) WITH (app application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L86	24	((secure) near2(internet)) SAME (app application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L87	64	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L88	110	((secure) near2(internet)) SAME	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM

L89	20	(app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) ((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:13 AM
L90	20	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:13 AM
L91	19	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:14 AM

L92	22966	ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data) (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/06 02:35 AM
L93	5	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)) AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:35 AM
L94	5	((US-20220279021-A1 OR US-20160135014- A1 OR US- 20090292815-A1 OR US-20090328197- A1).did. AND PGPB.dbnm.) OR ((US- 8839388-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/08/06 04:31 AM
L95	1	"20220279021"	(US-PGPUB)	OR	ON	ON	2024/08/06 04:35 AM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N2	1	((secure) near2(internet)) NEAR10 (app application) SAME ((communication ADJ	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:36 AM

N3	0	device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.) (((secure) near2(internet)) NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:36 AM
N4	0	(((secure) near2(internet)) NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) NEAR10 (id identifier identification identifying) SAME (wireless wirelessly)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:36 AM

N5	0	SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.) (((secure) near2(internet)) NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) NEAR10 (id identifier identification identifying) NEAR10 (wireless wirelessly) SAME (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:37 AM
N6	0	(((secure) near2(internet)) NEAR10 (app application) NEAR10 ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) NEAR10 (id identifier identification identifying) NEAR10 (wireless wirelessly) NEAR10 (data)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:37 AM
N7	0	((saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:40 AM

N8	0	(mobile ADJ terminal) ue) WITH (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)) AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:42 AM
N9	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:42 AM
N10	0	((saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate)) AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/08/06 02:42 AM
		((saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate)).CLM. AND (455/406.CCLS. G06F15/177.CPC. H04W28/0215.CPC.)					

Web Search History

date, time	web site	search string
8/6/2024 2:45:08 AM	Google Patents	Search Term 1 ((saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate))
8/6/2024 2:45:40 AM	Google Patents	Search Term 1 ((saved saving save stored storing store) ((device sensor) (credential)) (handheld (mobile device) (user terminal) (user equipment) cellphone smartphone (mobile terminal) ue) (network) (activate))
8/6/2024 2:45:43 AM	Google Patents	Search Term 1 ((saved saving stored storing store) ((device sensor) (credential)) (handheld (mobile device) (user terminal) (user equipment) cellphone smartphone (mobile terminal) ue) (network) (activate))
8/6/2024 2:47:05 AM	Google Patents	Search Term 1 ((saved saving stored storing store) ((device sensor) (credential)) ((mobile device) (user terminal) (user equipment) cellphone smartphone (mobile terminal) ue) (network) (activate))
8/6/2024 2:47:08 AM	Google Patents	Search Term 1 ((saved stored storing store) ((device sensor) (credential)) ((mobile device) (user terminal) (user equipment) cellphone smartphone (mobile terminal) ue) (network) (activate))
8/6/2024 2:47:13 AM	Google Patents	Search Term 1 ((saved stored storing store) ((device sensor) (credential)) ((mobile device) (user terminal) cellphone smartphone (mobile terminal) ue) (network) (activate))
8/6/2024 2:47:23 AM	Google Patents	Search Term 1 ((saved stored storing store) ((device sensor) (credential)) (cellphone smartphone (mobile terminal) ue) (network) (activate))
8/6/2024 2:47:31 AM	Google Patents	Search Term 1 ((saved stored storing store) ((device sensor) (credential)) (cellphone smartphone) (network) (activate))

date, time	web site	search string
-------------------	-----------------	----------------------

8/6/2024 2:47:54 AM	Google Patents	Search Term 1 ((saved stored storing store) ((device sensor) (credential)) (cellphone smartphone) (activate))
---------------------	-------------------	--



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :Zuriashwork Zenebe

Sale Accounting Date:08/21/2024

Sale Item Reference Number
17577237

Effective Date
06/19/2024

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20248K840277507	2806	SUBMISSION- INFORMATION DISCLOSURE STMT	\$104.00	Deposit Account



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: July 29, 2024

To: United States Patent and Trademark Office
Examiner: Murillo Garcia, Fabricio R.; Art Unit: 2633

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 2

Message:

Enclosed, please find Request for Continued Examination regarding Consideration of Response to Final Office Action + Pilot Request as filed on July 18, 2024.

Credit card payment in the amount of **\$544.00** as the required Request for Continued Examination fee is hereby included with this filing.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

<h2 style="margin: 0;">REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL</h2> <p style="font-size: small; margin: 10px 0;">Subsection (b) of 35 U.S.C. § 132, effective on May 29, 2000, provides for continued examination of an utility or plant application filed on or after June 8, 1995. See The American Inventors Protection Act of 1999 (AIPA).</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px 5px;">Application Number</td> <td style="padding: 2px 5px;">17/577,237</td> </tr> <tr> <td style="padding: 2px 5px;">Filing Date</td> <td style="padding: 2px 5px;">1/17/2022</td> </tr> <tr> <td style="padding: 2px 5px;">First Named Inventor</td> <td style="padding: 2px 5px;">Raleigh</td> </tr> <tr> <td style="padding: 2px 5px;">Group Art Unit</td> <td style="padding: 2px 5px;">2633</td> </tr> <tr> <td style="padding: 2px 5px;">Examiner Name</td> <td style="padding: 2px 5px;">Murillo Garcia, Fabricio R.</td> </tr> <tr> <td style="padding: 2px 5px;">Attorney Docket Number</td> <td style="padding: 2px 5px;">RALEP007C11C3C2C3C2C1C1C1</td> </tr> </table>	Application Number	17/577,237	Filing Date	1/17/2022	First Named Inventor	Raleigh	Group Art Unit	2633	Examiner Name	Murillo Garcia, Fabricio R.	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
Application Number	17/577,237												
Filing Date	1/17/2022												
First Named Inventor	Raleigh												
Group Art Unit	2633												
Examiner Name	Murillo Garcia, Fabricio R.												
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1												

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.

NOTE: 37 C.F.R. § 1.114 is effective on May 29, 2000. If the above-identified application was filed prior to May 29, 2000, applicant may wish to consider filing a continued prosecution application (CPA) under 37 C.F.R. § 1.53 (d) (PTO/SB/29) instead of a RCE to be eligible for the patent term adjustment provisions of the AIPA. See Changes to Application Examination and Provisional Application Practice, Final Rule, 65 Fed. Reg. 50092 (Aug. 16, 2000); Interim Rule, 65 Fed. Reg. 14865 (Mar. 20, 2000), 1233 Off. Gaz. Pat. Office 47 (Apr. 11, 2000), which established RCE practice.

1. **Submission required under 37 C.F.R. § 1.114**
 - a. ☒ Previously submitted
 - i. ☒ Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on July 18, 2024
(Any unentered amendment(s) referred to above will be entered).
 - ii. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
 - iii. ☐ Other _____
 - b. ☐ Enclosed
 - i. ☐ Amendment/Reply
 - ii. ☐ Affidavit(s)/Declaration(s)
 - iii. ☐ Information Disclosure Statement (IDS)
 - iv. ☐ Other _____
2. **Miscellaneous**
 - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months, Fee under 37 C.F.R. § 1.17(i) required)
 - b. ☐ Other _____
3. **Fees** The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed.
 - a. ☒ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 50-0731
 - i. ☒ RCE fee required under 37 C.F.R. § 1.17(e)
 - ii. ☒ Extension of time fee (37 C.F.R. §§ 1.136 and 1.17)
 - iii. ☐ Other _____
 - b. ☐ Check in the amount of \$ _____ enclosed.
 - c. ☒ Payment to be charged by Credit Card in the amount of **\$544.00**.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print/Type)	Farshad Farjani, Esq.	Registration No. (Attorney/Agent)	41,014
Signature	/Farshad Farjami/	Date	July 29, 2024

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: **Mail Stop RCE**, Commissioner For Patents, P. O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office on:

Name (Print/Type)	Evan C. Gunderman	Date	July 29, 2024
Signature	/evan c. gunderman/		



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 07/29/2024 07:16:13 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	66567879	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1 C1C1_RCE_July_29_24.pdf	2	-	68 KB
RALEP007C11C3C2C3C2C (1-1) 1C1C1_RCE_July_29_24- TRAN.LET.pdf	1	Transmittal Letter	31 KB
RALEP007C11C3C2C3C2C (2-2) 1C1C1_RCE_July_29_24- RCEX.pdf	1	Request for Continued Examination (RCE)	35 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C 1C1_RCE_July_29_24.pdf	ED2F5DA2C2F852FB583E46265EC9D97CDF1B94DD53DEE7F5 42F7445CCE70E797F2D9919673444190E0F623C2A830698DCC 1F81A1A7CC6B9D5E87E7225D613DAE
RALEP007C11C3C2C3C2C1C 1C1_RCE_July_29_24- TRAN.LET.pdf	0C8AA887124928FBFAFAD19601F595DC096650E74E4C185E1 1109B85AEBB4D1A1602A138F5F1B7F392D588EC5F1AF383628 6C542D9132B3587C021756196D04E
RALEP007C11C3C2C3C2C1C 1C1_RCE_July_29_24- RCEX.pdf	2F08A130950A554858BAFA808C2D5CCAE4D85407EB8BDB445 2C2A30C54F09A1F7127105E050864B7B5226E4F101E49F8A45 2EA8FD0C45116E0DDDD525567363

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 07/29/2024 07:16:13 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
-----------------------------	--	--

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	66567879	AUTHORIZED BY	Michael Farjami
CUSTOMER #	106963	FILING DATE	01/17/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Gregory G. Raleigh

Payment Information

PAYMENT METHOD CARD / 5006	PAYMENT TRANSACTION ID E20247SJ19527417	PAYMENT AUTHORIZED BY Evan Gunderman
PRE-AUTHORIZED ACCOUNT 500731	PRE-AUTHORIZED CATEGORY 37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees); 37 CFR 1.21 (Miscellaneous fees and charges)	

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2801	REQUEST FOR CONTINUED EXAMINATION (RCE) - 1ST REQUEST (SEE 37 CFR 1.114)	544.00	1	544.00
TOTAL AMOUNT:				\$544.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 17/577,237		Filing Date 01/17/2022		☐ To be Mailed	
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO									
APPLICATION AS FILED - PART I									
	(Column 1)	(Column 2)							
FOR	NUMBER FILED	NUMBER EXTRA			RATE (\$)			FEE (\$)	
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A			N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	1 minus 20 =	* 0			x \$50 =			0	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	* 0			x \$240 =			0	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))									
* If the difference in column 1 is less than zero, enter "0" in column 2.							TOTAL	0	
APPLICATION AS AMENDED - PART II									
	(Column 1)		(Column 2)	(Column 3)					
AMENDMENT	07/29/2024	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 15	Minus	** 20	= 0		x \$40 =	0	
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x \$192 =	0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
							TOTAL ADD'L FEE	0	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA			RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=		x \$0 =		
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x \$0 =		
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
							TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.							LIE		
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".							/GERALDINE L STANLEY/		
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".									
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.									

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850
106963	7590	07/26/2024		
Headwater Research LLC C/O Farjami & Farjami LLP 26522 La Alameda Ave., Suite 360 Mission Viejo, CA 92691			EXAMINER MURILLO GARCIA, FABRICIO R	
			ART UNIT 2633	PAPER NUMBER
			NOTIFICATION DATE 07/26/2024	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@farjami.com
ffarjami@farjami.com
patent@headwaterllc.com

Advisory Action Before the Filing of an Appeal Brief	Application No. 17/577,237		Applicant(s) Raleigh, Gregory G.	
	Examiner FABRICIO R MURILLO GARCIA		Art Unit 2633	AIA (FITF) Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 18 July 2024 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires _____ months from the mailing date of the prior Advisory Action or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANTS FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because

a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);

b) ☐ They raise the issue of new matter (see NOTE below);

c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: See Continuation Sheet (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☒ will not be entered; or (b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____

9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____

13. ☐ Note the attached Information *Disclosure Statement(s)*. (PTO/SB/08) Paper No(s). _____

14. ☐ Other: _____

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____

Claim(s) objected to: _____

Claim(s) rejected: 2-16.

Claim(s) withdrawn from consideration: _____

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

Continuation of 3. NOTE: Although claims have been amended, further consideration is needed to verify whether all of the previous objections and rejections have been overcome, and whether these current amendments do not raise new issues.

DO NOT ENTER: /F.M./

07/23/2024

Application Serial No.: 17/577,237
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh, Gregory G. Application Serial No.: 17/577,237 Filed: 1/17/2022 Title: Automated Device Provisioning and Activation	Group Art Unit: 2633 Examiner: Murillo Garcia, Fabricio R.
--	---

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This is in response to the *Final* Office Action, dated July 18, 2024, in the above-referenced patent application. Please enter and consider the following amendments and remarks.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: July 18, 2024

To: United States Patent and Trademark Office
Examiner: Murillo Garcia, Fabricio R.; Art Unit: 2633

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 9

Message:

Enclosed, please find the Amendment and Response to Final Office Action, dated July 18, 2024.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain PRIVILEGED AND CONFIDENTIAL information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 07/18/2024 05:32:34 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	66428361	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1 C1C1_Resp_to_Final_OA_Ju ly_18_24.pdf	9	-	68 KB
RALEP007C11C3C2C3C2C 1C1C1_Resp_to_Final_OA_ July_18_24-TRAN.LET.pdf	(1-1) 1	Transmittal Letter	30 KB
RALEP007C11C3C2C3C2C 1C1C1_Resp_to_Final_OA_ July_18_24-A.NE.pdf	(2-9) 8	Response After Final Action	50 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C 1C1_Resp_to_Final_OA_July_1 8_24.pdf	48AC41327F9798B8ECB69D0ED81C36ACA830BEBBB8418EA1 7614335F11AFA35D106995AE411D52366B5A383B9C5CDBFCE 396E1116D08BDAB7262695B7967D063
RALEP007C11C3C2C3C2C1C 1C1_Resp_to_Final_OA_July_1 8_24-TRAN.LET.pdf	3B18AAF613C6C86D7056942FC5F3079566826BEBEF894911E4 F18B4C1670EF28C444CDF1B9A4587013D52C4F49E5EF0AF0D F46D9B5081E2429339F49A67B9476
RALEP007C11C3C2C3C2C1C 1C1_Resp_to_Final_OA_July_1 8_24-A.NE.pdf	CC6C71933A9D1AF2547D5DA605991AE95C00DD6827157A1E9 C7E67DEB37FA939DD0AFDC5331ED823B510AEABDB0452C11 CDBDDA7F867535E9EB42625E109281D

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh, Gregory G. Application Serial No.: 17/577,237 Filed: 1/17/2022 Title: Automated Device Provisioning and Activation	Group Art Unit: 2633 Examiner: Murillo Garcia, Fabricio R.
--	---

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This is in response to the *Final* Office Action, dated July 18, 2024, in the above-referenced patent application. Please enter and consider the following amendments and remarks.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.

In the Claims:

Claim 1 (Cancelled)

Claim 2 (Currently Amended): A network message server adapted to communicate with a mobile end-user device having a plurality of applications, the network message server comprising:

one or more processors configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the received request corresponding to a first application of the plurality of application;

generate an Internet data message based on the received request, the Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and forwarding the application data in the transmitted Internet data message to the ~~mapped~~ first application mapped by the mobile end-user device to the first application identifier.

Claim 3 (Currently Amended): The network message server of claim 2, wherein the one or more processors are further configured to:

prior to transmitting, encrypt the ~~secure~~ generated Internet data message to generate encrypted ~~secure~~ Internet data message.

Claim 4 (Currently Amended): The network message server of claim 2, wherein the ~~secure~~ generated Internet data message is transmitted using one or more of encryption on a transport services stack, ~~IP (Internet Protocol)~~ Internet Protocol (IP) layer encryption, or tunneling.

Claim 5 (Previously Presented): The network message server of claim 2, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 6 (Currently Amended): The network message server of claim 2, wherein the one or more processors are further configured to:
authenticate the first application prior to transmitting the generated Internet data message to the mobile end-user device.

Claim 7 (Currently Amended): A method for use by a network message server adapted to communicate with a mobile end-user device having a plurality of applications, the method comprising:

providing a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receiving a request to transmit application data, the received request corresponding to a first application of the plurality of application;

generating an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and

transmitting, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the

transmitted Internet data message to the first application corresponding to the first application identifier, and forwarding the application data in the transmitted Internet data message to the ~~mapped~~ first application mapped by the mobile end-user device to the first application identifier.

Claim 8 (Currently Amended): The method of claim 7, further comprising:
prior to transmitting, encrypting the ~~secure~~ generated Internet data message to generate encrypted ~~secure~~ Internet data message.

Claim 9 (Currently Amended): The method of claim 7, wherein the ~~secure~~ generated Internet data message is transmitted using one or more of encryption on a transport services stack, ~~IP (Internet Protocol)~~ Internet Protocol (IP) layer encryption, or tunneling.

Claim 10 (Previously Presented): The method of claim 7, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 11 (Currently Amended): The method of claim 7, further comprising:
authenticating the first application prior to transmitting the generated Internet data message to the mobile end-user device.

Claim 12 (Currently Amended): A network system comprising:
a mobile end-user device having a plurality of applications;
a network message server adapted to communicate with the mobile end-user device, the network message server configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the received request corresponding to a first application of the plurality of application;

generate an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device;

the mobile end-user device configured to:

receive the transmitted Internet data message from the network message server;

map the first application identifier included in the received Internet data message to the first application corresponding to the first application identifier; and

forward ~~forwarding~~ the application data in the received Internet data message to the ~~mapped~~ first application mapped by the mobile end-user device to the first application identifier.

Claim 13 (Currently Amended): The network system of claim 12, wherein the network message server is further configured to:

prior to transmitting, encrypt the ~~secure~~ generated Internet data message to generate encrypted ~~secure~~ Internet data message.

Claim 14 (Currently Amended): The network system of claim 12, wherein the ~~secure~~ generated Internet data message is transmitted using one or more of encryption on a transport services stack, ~~IP (Internet Protocol)~~ Internet Protocol (IP) layer encryption, or tunneling.

Claim 15 (Previously Presented): The network system of claim 12, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 16 (Currently Amended): The network system of claim 12, wherein the network message server is further configured to:

authenticate the first application prior to transmitting the generated Internet data message to the mobile end-user device.

REMARKS

The *Final* Office Action, dated July 18, 2024 (“Office Action”), rejected claims 2-16. By the present response, Applicant amends claims 2-4, 6-9, 11-14 and 16. No new matter is added. Thus, after the present response, claims 2-16 remain pending in the present application. Applicant respectfully requests allowance of claims 2-16 in view of the following remarks.

A. Claim Objections

The Office Action objected to claims 2, 4, 7, 9, 12 and 14. Although Applicant does not believe that the suggested changes are needed, without acquiescence and to advance prosecution of the present application, Applicant has amended claims 2, 4, 7, 9, 12 and 14 to overcome the objection.

B. 35 U.S.C. § 112(b)

The Office Action rejected claims 2-16, under 35 U.S.C. § 112(b), as being indefinite. By the present amendment, Applicant has amended claims 2, 3, 4, 7-9 and 12-14 to overcome the rejection of claims 2-16, under 35 U.S.C. § 112(b).

C. Conclusion

Based on the foregoing reasons, Applicant respectfully requests allowance of claims 2-16 pending in the present application.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.

Respectfully Submitted,
FARJAMI & FARJAMI LLP

/Farshad Farjami/
Farshad Farjami
Reg. No. 41,014

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, California 92691
Telephone: (949) 282-1000
Facsimile: (949) 282-1002

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

July 18, 2024
Date

Evan C. Gunderman
Name

/evan c. gunderman/
Signature

In the Claims:

Claim 1 (Cancelled)

Claim 2 (Currently Amended): A network message server adapted to communicate with a mobile end-user device having a plurality of applications, the network message server comprising:

one or more processors configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the received request corresponding to a first application of the plurality of application;

generate an Internet data message based on the received request, the Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the transmitted Internet data message to the first application corresponding to the first application identifier, and forwarding the application data in the transmitted Internet data message to the ~~mapped~~ first application mapped by the mobile end-user device to the first application identifier.

Claim 3 (Currently Amended): The network message server of claim 2, wherein the one or more processors are further configured to:

prior to transmitting, encrypt the ~~secure~~ generated Internet data message to generate encrypted ~~secure~~ Internet data message.

Claim 4 (Currently Amended): The network message server of claim 2, wherein the ~~secure~~ generated Internet data message is transmitted using one or more of encryption on a transport services stack, ~~IP (Internet Protocol)~~ Internet Protocol (IP) layer encryption, or tunneling.

Claim 5 (Previously Presented): The network message server of claim 2, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 6 (Currently Amended): The network message server of claim 2, wherein the one or more processors are further configured to:
authenticate the first application prior to transmitting the generated Internet data message to the mobile end-user device.

Claim 7 (Currently Amended): A method for use by a network message server adapted to communicate with a mobile end-user device having a plurality of applications, the method comprising:

providing a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receiving a request to transmit application data, the received request corresponding to a first application of the plurality of application;

generating an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and

transmitting, over the secure Internet data connection, the generated Internet data message to the mobile end-user device for mapping the first application identifier included in the

transmitted Internet data message to the first application corresponding to the first application identifier, and forwarding the application data in the transmitted Internet data message to the ~~mapped~~ first application mapped by the mobile end-user device to the first application identifier.

Claim 8 (Currently Amended): The method of claim 7, further comprising:
prior to transmitting, encrypting the ~~secure~~ generated Internet data message to generate encrypted ~~secure~~ Internet data message.

Claim 9 (Currently Amended): The method of claim 7, wherein the ~~secure~~ generated Internet data message is transmitted using one or more of encryption on a transport services stack, ~~IP (Internet Protocol)~~ Internet Protocol (IP) layer encryption, or tunneling.

Claim 10 (Previously Presented): The method of claim 7, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 11 (Currently Amended): The method of claim 7, further comprising:
authenticating the first application prior to transmitting the generated Internet data message to the mobile end-user device.

Claim 12 (Currently Amended): A network system comprising:
a mobile end-user device having a plurality of applications;
a network message server adapted to communicate with the mobile end-user device, the network message server configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the received request corresponding to a first application of the plurality of application;

generate an Internet data message based on the received request, the generated Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the generated Internet data message to the mobile end-user device;

the mobile end-user device configured to:

receive the transmitted Internet data message from the network message server;

map the first application identifier included in the received Internet data message to the first application corresponding to the first application identifier; and

forward ~~forwarding~~ the application data in the received Internet data message to the ~~mapped~~ first application mapped by the mobile end-user device to the first application identifier.

Claim 13 (Currently Amended): The network system of claim 12, wherein the network message server is further configured to:

prior to transmitting, encrypt the ~~secure~~ generated Internet data message to generate encrypted ~~secure~~ Internet data message.

Claim 14 (Currently Amended): The network system of claim 12, wherein the ~~secure~~ generated Internet data message is transmitted using one or more of encryption on a transport services stack, ~~IP (Internet Protocol)~~ Internet Protocol (IP) layer encryption, or tunneling.

Claim 15 (Previously Presented): The network system of claim 12, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 16 (Currently Amended): The network system of claim 12, wherein the network message server is further configured to:

authenticate the first application prior to transmitting the generated Internet data message to the mobile end-user device.

REMARKS

The *Final* Office Action, dated July 18, 2024 (“Office Action”), rejected claims 2-16. By the present response, Applicant amends claims 2-4, 6-9, 11-14 and 16. No new matter is added. Thus, after the present response, claims 2-16 remain pending in the present application. Applicant respectfully requests allowance of claims 2-16 in view of the following remarks.

A. Claim Objections

The Office Action objected to claims 2, 4, 7, 9, 12 and 14. Although Applicant does not believe that the suggested changes are needed, without acquiescence and to advance prosecution of the present application, Applicant has amended claims 2, 4, 7, 9, 12 and 14 to overcome the objection.

B. 35 U.S.C. § 112(b)

The Office Action rejected claims 2-16, under 35 U.S.C. § 112(b), as being indefinite. By the present amendment, Applicant has amended claims 2, 3, 4, 7-9 and 12-14 to overcome the rejection of claims 2-16, under 35 U.S.C. § 112(b).

C. Conclusion

Based on the foregoing reasons, Applicant respectfully requests allowance of claims 2-16 pending in the present application.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.

Respectfully Submitted,
FARJAMI & FARJAMI LLP

/Farshad Farjami/
Farshad Farjami
Reg. No. 41,014

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, California 92691
Telephone: (949) 282-1000
Facsimile: (949) 282-1002

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

July 18, 2024
Date

Evan C. Gunderman
Name

/evan c. gunderman/
Signature



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850
106963	7590	07/18/2024		
Headwater Research LLC C/O Farjami & Farjami LLP 26522 La Alameda Ave., Suite 360 Mission Viejo, CA 92691			EXAMINER MURILLO GARCIA, FABRICIO R	
			ART UNIT 2633	PAPER NUMBER
			NOTIFICATION DATE 07/18/2024	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@farjami.com
ffarjami@farjami.com
patent@headwaterllc.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Response to Arguments

Following response to arguments is based on Applicant's arguments filed on **04 June 2024**.

Regarding Previous Double Patenting Rejection

Previous rejection of claim 1 has been withdrawn in view of the cancelation of the rejected claim.

Regarding Previous Rejection Under 35 USC § 102

Previous rejection of claim 1 has been withdrawn in view of the cancelation of the rejected claim.

Claim Status

Claim 1 has been canceled. Claims 2-16 have been added. Thus, claims 2-16 are presented for examination.

Information Disclosure Statement

The IDS submitted on 19 June 2023 is in compliance and has been considered.

Examiner notes that, given the quantity and length of the references, only a cursory review has been performed until such time as Applicant provides a detailed explanation of relevance or specifically points out only those sections of relevance in the disclosure.

Claim Objections

Claims 2, 4, 7, 9, 12, 14 are objected to because of the following informalities:

For claim 2:

At line 6, it should be “*application data, the received request*”.

At line 8, it should be “*based on the received request, the generated Internet data message*”.

At line 11, it should be “*Internet data connection, the generated Internet data message*”.

At line 12, it should be “*included in the generated Internet*”.

At line 14, it should be “*in the generated Internet*”.

For claim 4:

At lines 2-3, it should be “Internet Protocol (IP)”.

For claim 7:

At line 5, it should be “*application data, the received request*”.

At line 7, it should be “*based on the received request, the generated Internet*”.

data message".

At line 10, it should be "*Internet data connection, the generated Internet data message*".

At line 11, it should be "*included in the generated Internet*".

At line 13, it should be "*in the generated Internet*".

For claim 9:

At line 2, it should be "Internet Protocol (IP)".

For claim 12:

At line 7, it should be "*application data, the received request*".

At line 9, it should be "*based on the received request, the generated Internet data message*".

At line 12, it should be "*Internet data connection, the generated Internet data message*".

At line 15, it should be "*received the transmitted Internet data message*".

At line 16, it should be "*in the generated Internet*".

At line 17, it should be "*in the generated Internet*".

For claim 14:

At lines 2-3, it should be "Internet Protocol (IP)".

Appropriate correction is required.

Claim Rejections - 35 USC § 112 – Second Paragraph

The following is a quotation of 35 U.S.C. 112(b):

(B) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2-16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

For claim 2:

At line 14, “the mapped application” lacks of antecedent basis as there is no previous recitation of “*a mapped application*”.

For claim 3:

At line 3, “the secure Internet data message” lacks of antecedent basis.

For claim 4:

At lines 1-2, “the secure Internet data message” lacks of antecedent basis.

For claim 7:

At line 14, “the mapped application” lacks of antecedent basis as there is no

previous recitation of “*a mapped application*”.

For claim 8:

At line 2, “the secure Internet data message” lacks of antecedent basis.

For claim 9:

At line 1, “the secure Internet data message” lacks of antecedent basis.

For claim 12:

At line 18, “the mapped application” lacks of antecedent basis as there is no previous recitation of “*a mapped application*”.

For claim 13:

At line 3, “the secure Internet data message” lacks of antecedent basis.

For claim 14:

At line 1, “the secure Internet data message” lacks of antecedent basis.

For claims 3-6, 8-11, 13-16:

These claims are also rejected as they depend upon a rejected claim.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FABRICIO R MURILLO GARCIA whose telephone number is (571)270-5708. The examiner can normally be reached 9-5pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sam K Ahn can be reached on 5712723044. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is

available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

July 13, 2024

/FABRICIO R MURILLO GARCIA/
Primary Examiner, Art Unit 2633

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC - Searched*		
Symbol	Date	Examiner
G06F15/177	03/09/2024	FM
H04W28/0215	03/09/2024	FM

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
455/406		03/09/2024	FM

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
East (See Attachment)	03/09/2024	FM
Inventor Search (search for double patenting)	03/09/2024	FM
Non Patentable Literature	03/09/2024	FM
455/406 - See Attached East Search	03/09/2024	FM
G06F15/177 - See Attached East Search	03/09/2024	FM
H04W28/0215 - See Attached East Search	03/09/2024	FM
Updated	06/25/2024	FM

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

Web Search History

date, time	web site	search string
6/25/2024 3:19:53 AM	Google Patents	Search Term 1 ((secure) near2(internet)) same (app application) same ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) same (id identifier identification identifying) same (wireless wirelessly) same (data)
6/25/2024 3:20:49 AM	Google Patents	Search Term 1 ((secure) (internet)) (app application) ((communication device) (user terminal) (user equipment) (user device) (electronic terminal) (electronic device) handheld cellphone smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)
6/25/2024 3:21:12 AM	Google Patents	Search Term 1 ((secure)) (app application) ((communication device) (user terminal) (user equipment) (user device) (electronic terminal) (electronic device) handheld cellphone smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)
6/25/2024 3:21:20 AM	Google Patents	Search Term 1 ((secure)) (app application) ((communication device) (user equipment) (user device) (electronic terminal) (electronic device) handheld cellphone smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)
6/25/2024 3:21:25 AM	Google Patents	Search Term 1 ((secure)) (app application) ((communication device) (electronic terminal) (electronic device) handheld cellphone smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)
6/25/2024 3:21:31 AM	Google Patents	Search Term 1 ((secure)) (app application) ((communication device) (electronic device) handheld cellphone smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)

date, time	web site	search string
6/25/2024 3:21:34 AM	Google Patents	Search Term 1 ((secure)) (app application) ((communication device) (electronic device) handheld smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)
6/25/2024 3:21:40 AM	Google Patents	Search Term 1 ((secure)) (app application) ((electronic device) handheld smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)
6/25/2024 3:21:48 AM	Google Patents	Search Term 1 ((secure)) ((electronic device) handheld smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)
6/25/2024 3:21:53 AM	Google Patents	Search Term 1 ((electronic device) handheld smartphone ue (mobile terminal) (mobile device)) (id identifier identification identifying) (wireless wirelessly) (data)

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	1	"17577237"	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:06 AM
L2	633	((("RALEIGH") near3 ("Gregory"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/03/09 06:10 AM
L3	1	((US-20220279021-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:19 PM
L4	3098	(store) WITH ((device) near2 (credential))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:36 PM
L5	2	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L6	0	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal) WITH (activate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L7	30	("6178511" "6243816" "7249182" "7296036" "7310515" "7346855" "7353462" "8472874" "8606854" "20040009750" "20040113807" "20050026594" "20050076124" "20050193093" "20050281237" "20060063548" "20060234631" "20070021111" "20070167136" "20070168425" "20070242814" "20070260751" "20080051033" "20080108308" "20090209202").pn. OR ("9357352").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:38 PM
L8	4	((US-11304026-B2 OR US-10963844-B2 OR US-10250549-B2 OR US-9609673-B2).did. AND USPT.dbnm.)	(USPAT)	OR	ON	ON	2024/03/09 06:38 PM
L9	4	((US-8606854-B2 OR US-8472874-B2).did.	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM

L10	4	AND USPT.dbnm.) OR ((US-20090209202-A1 OR US-20080108308- A1).did. AND PGPB.dbnm.) ((US-7353462-B2 OR US-7346855-B2 OR US-7296036-B2).did. AND USPT.dbnm.) OR ((US-20080051033- A1).did. AND PGPB.dbnm.)	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L11	4	((US-20070260751-A1 OR US-20070242814- A1 OR US- 20070167136-A1 OR US-20070168425- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L12	4	((US-20070021111-A1 OR US-20060234631- A1 OR US- 20060063548-A1 OR US-20050281237- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L13	41	("6867733" "7418268" "7686217" "7847684" "8010131" "8108414" "8655385" "8688143" "8892130" "9173245" "9203857" "9226105" "9268920" "9357352" "9485211" "9830562" "9940402" "10013489" "10049400" "10075822" "10078696" "10264609" "10575138" "10599390" "20040116106" "20100313142" "20130316735" "20130331087" "20140162698" "20150058427" "20150080027" "20150088672" "20150365787" "20150378587" "20160261985" "20160334545" "20160364811" "20180176166"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:39 PM

L14	2	"20190014220" "20190215660" "20210173880").pn. OR ("11304026").urpn. AND (PGPB USPT USOC).dbnm. (storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L15	5	(stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L16	5	(save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L17	5	(saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L18	5	(saved saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L19	6	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L20	30	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L21	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L22	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM

L23	72	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L24	75	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L25	759	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L26	762	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L27	128	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L28	88	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L29	78	(user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L30	66	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L31	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L32	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activae)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L33	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L34	1	(user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L35	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L36	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start begin)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:44 PM
L37	1	("2022/0124167").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:45 PM
L38	2	((US-20220279021-A1 OR US-20160135014- A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/03/09 06:45 PM
L39	1	(saved saving save stored storing store) near10 ((device sensor)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L40	1	near2 (credential) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L41	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L42	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began began begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L43	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L44	1	near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L45	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L46	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L47	4	starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) WITH ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L48	3	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L49	4	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L50	15	(saved saving save	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09

		stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) WITH (initiated initiating running starting run activate initiate start started began begun begin beginning)					06:56 PM
L51	4	((US-20220124167-A1 OR US-20200275225- A1 OR US- 20170006034-A1).did. AND PGPB.dbnm.) OR ((US-9554061-B1).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:59 PM
L52	3	((US-20140373012-A1 OR US-20140337940- A1 OR US- 20130191885-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:59 PM
L53	24	("6757837" "6882712" "6889510" "7355730" "20020082924" "20060236325" "20070225828" "20080167127" "20080167128" "20080167133" "20090078760" "20100112997" "20100268401" "20110113087" "20110202798" "20110294466" "20120129492" "20120221893" "20120226619" "20120324067" "20140028449" "20140173059").pn. OR ("9129127").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM
L54	88	("6564056" "7664707" "7908401" "8311513" "8447696" "8974544" "9129127" "9141150" "9183380" "9204298" "9246921" "9489250"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM

		"9507950" "9524174" "9531559" "9575477" "20040125782" "20050246243" "20080062258" "20080204199" "20090023395" "20100031371" "20100094981" "20110145927" "20130067551" "20130171981" "20130191885" "20130254437" "20130304795" "20130311684" "20140040989" "20140098247" "20140245765" "20140263612" "20140266669" "20140266679" "20140277597" "20140279109" "20140282486" "20140304632" "20140313048" "20140344454" "20140359042" "20140376528" "20150006686" "20150033305" "20150038129" "20150040246" "20150052578" "20150061859" "20150081928" "20150097689" "20150100618" "20150109104" "20150160935" "20150163412" "20150177705" "20150198938" "20150215337" "20150222578" "20150261954" "20150279134" "20150304171" "20150309548" "20150324179" "20150364028" "20160014108" "20160063854" "20160098362" "20160099972" "20160103494" "20160109864"				
--	--	--	--	--	--	--

		"20160119742" "20160142258" "20160142532" "20160294602" "20160337945" "20160351036" "20160380987" "20170019264" "20170034156" "20170034158" "20170046173" "20170048712" "20170078298" "20170093860" "20170099560" "20170109998").pn. OR ("10157271").urpn. AND (PGPB USPT USOC).dbnm.					
L55	4	((US-20170109998-A1 OR US-20170099560- A1 OR US- 20170093860-A1).did. AND PGPB.dbnm.) OR ((US-9575477-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:00 PM
L56	1	((US-20160135014- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 07:37 PM
L57	1	"8839388".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:49 PM
L58	1	"9037127".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:54 PM
L59	1	"9232403".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:56 PM
L60	1	"9532161".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:57 PM
L61	1	"9641957".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:58 PM
L62	1	"10321320".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:59 PM
L63	1	"11228617".pn.	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 08:00 PM
L64	8	"20090292815"	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 08:06 PM
L65	1	((US-20090292815- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 09:27 PM
L66	806072	(memory WITH instructions) AND ;65	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 09:27 PM
L67	0	(memory WITH instructions) AND L65	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 09:27 PM
L68	1	(memory SAME	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09

L69	2126	instructions) AND L65 ((secure) near2(internet)) WITH (application)	(US-PGPUB; USPAT)	OR	ON	ON	09:28 PM 2024/06/25 03:05 AM
L70	7	((secure) near2(internet)) WITH (application) WITH (communication ADJ device)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L71	8	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L72	14	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:07 AM
L73	56	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:08 AM
L74	78	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L75	90	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L76	90	((secure) near2(internet)) WITH (application) WITH	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM

L77	103	((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld cellphone))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L78	103	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) (handheld cellphone smartphone))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:09 AM
L79	103	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal))	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L80	144	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM

L81	3	terminal) (mobile ADJ device)) ((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L82	12	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L83	16	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM
L84	16	((secure) near2(internet)) WITH (application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:10 AM

L85	16	cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying) ((secure) near2(internet)) WITH (app application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L86	24	((secure) near2(internet)) SAME (app application) WITH ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L87	64	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) WITH (id identifier identification identifying)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM
L88	110	((secure) near2(internet)) SAME	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:12 AM

L89	20	(app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) ((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:13 AM
L90	20	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:13 AM
L91	19	((secure) near2(internet)) SAME (app application) SAME ((communication ADJ device) (user ADJ terminal) (user ADJ equipment) (user ADJ device) (electronic ADJ terminal) (electronic ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly)	(US-PGPUB; USPAT)	OR	ON	ON	2024/06/25 03:14 AM

		ADJ device) handheld cellphone smartphone ue (mobile ADJ terminal) (mobile ADJ device)) SAME (id identifier identification identifying) SAME (wireless wirelessly) SAME (data)					
--	--	--	--	--	--	--	--

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

PATENT
RALEP007C11C3C2C3C2C1C1C1**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of: Raleigh, Gregory	Examiner: NOT YET ASSIGNED
Serial No.: 17/577,237	Art Unit: 2414
Filed: January 17, 2022	Conf. No.: 5850
Title: Automated Device Provisioning and Activation	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

The references cited on attached form PTO/SB/08A are being called to the attention of the Examiner. Copies of the references are not enclosed.

In accordance with 37 CFR §1.98(d), copies of the references can be found in related U.S. Patent Application No. 16/436,628 filed June 10, 2019, of which the instant application is a continuation, or in related U.S. Patent Application No. 15/582,350 filed on April 28, 2017, of which 16/436,628 is a continuation.

It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

PATENT
RALEP007C11C3C2C3C2C1C1C1

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement, but if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No.

50-0731.

Respectfully submitted,
Farjami & Farjami LLP

Date: May 23, 2022

By: /Farshad Farjami/
Farshad Farjami, Esq.
Reg. No. 41,014

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691
Tel: (949) 282-1000
Fax: (949) 282-1002

<u>CERTIFICATE OF ELECTRONIC TRANSMISSION</u>	
I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.	
<u>May 24, 2022</u>	
Date	
<u>Evan C. Gunderman</u>	<u>/evan c. gunderman /</u>
Name	Signature

Doc code: IDS

PTO/SB/08a (01-22)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	10027819	B2	2018-07-17	Lu et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20010048738	A	2001-12-06	Baniak, Paul G. et al.	
	2	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	3	20020013844	A1	2002-01-31	Garrett et al.	
	4	20020022472		2002-02-21	WATLER et al.	
	5	20020022483	A1	2002-02-21	Thompson et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

6	20020049074	A	2002-04-25	Eisinger, Bernd et al.	
7	20020099848	A1	2002-07-25	Lee, Hoon	
8	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	
9	20020120370	A1	2002-08-29	Parupudi et al.	
10	20020120540		2002-08-29	KENDE et al.	
11	20020131404		2002-09-19	MEHTA et al.	
12	20020138599	A1	2002-09-26	Dilman et al.	
13	20020138601		2002-09-26	PIPONIUS et al.	
14	20020154751	A1	2002-10-24	Thompson et al.	
15	20020161601	A	2002-10-31	Nauer, Bernhard et al.	
16	20020164983		2002-11-07	Raviv, Li-On et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

17	20020176377		2002-11-28	HAMILTON, Thomas E.	
18	20020188732	A1	2002-12-12	Buckman et al.	
19	20020191573	A1	2002-12-19	Whitehill et al.	
20	20020199001		2002-12-26	WENOCUR et al.	
21	20030004937		2003-01-02	SALMENKAITA et al.	
22	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
23	20030013434		2003-01-16	ROSENBERG et al.	
24	20030018524		2003-01-23	FISHMAN et al.	
25	20030028623	A1	2003-02-06	Hennessey et al.	
26	20030046396		2003-03-06	RICHTER et al.	
27	20030050070		2003-03-13	MASHINSKY et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	28	20030050837		2003-03-13	KIM, Do Sik	
	29	20030084321	A1	2003-05-01	Tarquini et al.	
	30	20030088671	A1	2003-05-08	Klinker et al.	
	31	20030133408		2003-07-17	CHENG et al.	
	32	20030134650	A1	2003-07-17	Sundar et al.	
	33	20030159030	A1	2003-08-21	Evans, Junius A.	
	34	20030161265		2003-08-28	CAO et al.	
	35	20030171112		2003-09-11	Lupper, Alfred et al.	
	36	20030182420		2003-09-25	JONES et al.	
	37	20030182435		2003-09-25	REDLICH et al.	
	38	20030184793	A1	2003-10-02	Pineau, Richard A.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

39	20030188006	A	2003-10-02	Bard, Steven R.	
40	20030188117	A	2003-10-02	Yoshino et al.	
41	20030220984		2003-11-27	JONES et al.	
42	20030224781		2003-12-04	MILFORD et al.	
43	20030229900		2003-12-11	REISMAN, Richard	
44	20030233332	A	2003-12-18	Keeler, James D. et al.	
45	20030236745		2003-12-25	HARTSELL et al.	
46	20040019539		2004-01-29	RAMAN et al.	
47	20040019564	A1	2004-01-29	Goldthwaite et al.	
48	20040021697		2004-02-05	BEATON et al.	
49	20040024756	A1	2004-02-05	Rickard, John Terrell	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

50	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
51	20040039792	A1	2004-02-26	Nakanishi, Tornoaki	
52	20040044623		2004-03-04	WAKE et al.	
53	20040047358		2004-03-11	CHEN et al.	
54	20040054779	A1	2004-03-18	Takeshima et al.	
55	20040073672		2004-04-15	FASCENDA, Anthony C.	
56	20040082346		2004-04-29	SKYTT et al.	
57	20040098715		2004-05-20	AGHERA et al.	
58	20040102182	A	2004-05-27	Reith, Lothar et al.	
59	20040103193		2004-05-27	PANDYA et al.	
60	20040107360		2004-06-03	HERRMANN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	61	20040116140	A1	2004-06-17	Babbar et al.	
	62	20040127200		2004-07-01	SHAW et al.	
	63	20040127208	A1	2004-07-01	Nair et al.	
	64	20040127256	A1	2004-07-01	Goldthwaite et al.	
	65	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	66	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	67	20040137890	A1	2004-07-15	Kalke, Catherine	
	68	20040165596	A1	2004-08-26	Garcia et al.	
	69	20040167958	A1	2004-08-26	Stewart et al.	
	70	20040168052		2004-08-26	CLISHAM et al.	
	71	20040170191	A	2004-09-02	Guo et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

72	20040176104	A1	2004-09-09	Arcens	
73	20040198331		2004-10-07	COWARD et al.	
74	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
75	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
76	20040225561	A1	2004-11-11	Hertzberg et al.	
77	20040225898	A	2004-11-11	Frost, D. et al.	
78	20040236547		2004-11-25	RAPPAPORT et al.	
79	20040243680	A1	2004-12-02	Mayer, Georg	
80	20040243992	A	2004-12-02	Gustafson et al.	
81	20040249918		2004-12-09	SUNSHINE, Roger N.	
82	20040255145	A	2004-12-16	Chow, Jerry	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

83	20040259534	A1	2004-12-23	Chaudhari et al.	
84	20040260766	A1	2004-12-23	Barros et al.	
85	20040267872	A1	2004-12-30	Serdy et al.	
86	20050007993		2005-01-13	Chambers, Mahdi et al.	
87	20050009499		2005-01-13	KOSTER, Karl	
88	20050021995		2005-01-27	LAL et al.	
89	20050041617	A1	2005-02-24	Huotari et al.	
90	20050048950		2005-03-03	MORPER, Hans-Jochen	
91	20050055291		2005-03-10	BEVENTE et al.	
92	20050055309		2005-03-10	WILLIAMS et al.	
93	20050055595	A	2005-03-10	Frazer et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

94	20050060266		2005-03-17	DEMELLO et al.	
95	20050060525	A1	2005-03-17	Schwartz et al.	
96	20050075115	A1	2005-04-07	Cornelle et al.	
97	20050079863	A	2005-04-14	Macaluso, Anthony G.	
98	20050091505	A1	2005-04-28	Riley et al.	
99	20050096024	A1	2005-05-05	Bicker et al.	
100	20050097516		2005-05-05	DONNELLY et al.	
101	20050107091		2005-05-19	VANNITHAMBY et al.	
102	20050108075	A1	2005-05-19	Douglas et al.	
103	20050111463	A1	2005-05-26	Leung et al.	
104	20050128967		2005-06-16	SCOBIE, Donald MacGregor	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	105	20050135264	A1	2005-06-23	Popoff et al.	
	106	20050163320	A1	2005-07-28	Brown et al.	
	107	20050166043		2005-07-28	ZHANG et al.	
	108	20050183143		2005-08-18	ANDERHOLM et al.	
	109	20050186948	A	2005-08-25	Gallagher et al.	
	110	20050198377		2005-09-08	FERGUSON et al.	
	111	20050216421		2005-09-29	BARRY et al.	
	112	20050228985		2005-10-13	YLIKOSKI et al.	
	113	20050238046		2005-10-27	HASSAN et al.	
	114	20050239447	A1	2005-10-27	Holzman et al.	
	115	20050245241	A1	2005-11-03	Durand et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

116	20050246282		2005-11-03	NASLUND et al.	
117	20050250508		2005-11-10	GUO et al.	
118	20050250536	A1	2005-11-10	Deng et al.	
119	20050254435		2005-11-17	MOAKLEY et al.	
120	20050266825		2005-12-01	CLAYTON, Steve	
121	20050266880		2005-12-01	GUPTA, Vivek G.	
122	20060014519		2006-01-19	MARSH et al.	
123	20060019632		2006-01-26	CUNNINGHAM et al.	
124	20060020787	A1	2006-01-26	Choyi et al.	
125	20060026679	A1	2006-02-02	Zakas	
126	20060030306	A1	2006-02-09	Kuhn, Brian Gerald	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

127	20060034256		2006-02-16	ADDAGATLA et al.	
128	20060035631	A1	2006-02-16	White et al.	
129	20060040642		2006-02-23	BORIS et al.	
130	20060045245		2006-03-02	AARON et al.	
131	20060048223		2006-03-02	LEE et al.	
132	20060068796	A	2006-03-30	Millen, Stephanie L. et al.	
133	20060072451	A1	2006-04-06	Ross, Alan D.	
134	20060072550	A1	2006-04-06	Davis et al.	
135	20060072646		2006-04-06	FEHER, Kamilo	
136	20060075506	A1	2006-04-06	Sanda et al.	
137	20060085543		2006-04-20	HRASTAR et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

138	20060095517	A1	2006-05-04	O'Connor et al.	
139	20060098627	A1	2006-05-11	Karaoguz et al.	
140	20060099970	A1	2006-05-11	Morgan et al.	
141	20060101507	A1	2006-05-11	Camenisch, Ja L.	
142	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
143	20060114821	A1	2006-06-01	Willey et al.	
144	20060114832	A	2006-06-01	Hamilton et al.	
145	20060126562	A1	2006-06-15	Liu, Huitao	
146	20060135144	A	2006-06-22	Jothipragasam, Premkumar	
147	20060136882	A1	2006-06-22	Noonan et al.	
148	20060143066	A1	2006-06-29	Calabria	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

149	20060143098		2006-06-29	LAZARIDIS, Mihal	
150	20060156398	A	2006-07-13	Ross et al.	
151	20060160536	A	2006-07-20	Chou, Joey	
152	20060165060		2006-07-27	DUA, Robin	
153	20060168128	A	2006-07-27	Sistla et al.	
154	20060173959	A	2006-08-03	Mckelvie et al.	
155	20060174035	A	2006-08-03	Tufail, Mudassir	
156	20060178917		2006-08-10	MERRIAM et al.	
157	20060178918		2006-08-10	MIKURAK, Michael G.	
158	20060182137	A1	2006-08-17	Zhou et al.	
159	20060183462		2006-08-17	KOLEHMAINEN, Mikko	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	160	20060190314		2006-08-24	HERNANDEZ, Rick	
	161	20060190987	A1	2006-08-24	Ohta et al.	
	162	20060193280	A1	2006-08-31	Lee et al.	
	163	20060199608		2006-09-07	DUNN et al.	
	164	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	165	20060206709	A1	2006-09-14	Labrou et al.	
	166	20060206904		2006-09-14	WATKINS et al.	
	167	20060218395		2006-09-28	MAES, Stephane H.	
	168	20060233108		2006-10-19	KRISHNAN, Murali R.	
	169	20060233166		2006-10-19	BOU-DIAB et al.	
	170	20060236095		2006-10-19	SMITH et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

171	20060242685		2006-10-26	HEARD et al.	
172	20060258341		2006-11-16	MILLER et al.	
173	20060277590	A1	2006-12-07	Limont et al.	
174	20060291419	A1	2006-12-28	McConnell et al.	
175	20060291477		2006-12-28	CROAK et al.	
176	20070005795	A1	2007-01-04	Gonzalez, Ruben	
177	20070019670		2007-01-25	FALARDEAU, Eric	
178	20070022289		2007-01-25	ALT et al.	
179	20070025301	A	2007-02-01	Petersson et al.	
180	20070033194	A	2007-02-08	Srinivas et al.	
181	20070033197	A	2007-02-08	Scherzer, Shimon et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

182	20070036312		2007-02-15	CAI et al.	
183	20070055694		2007-03-08	RUGE et al.	
184	20070060200	A1	2007-03-15	Boris et al.	
185	20070061243	A1	2007-03-15	Ramer et al.	
186	20070061800	A1	2007-03-15	Cheng et al.	
187	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
188	20070073899	A1	2007-03-29	Judge et al.	
189	20070076616		2007-04-05	NGO et al.	
190	20070093243		2007-04-26	KAPADEKAR et al.	
191	20070100981		2007-05-03	ADAMCZYK et al.	
192	20070101426		2007-05-03	LEE et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	193	20070104126		2007-05-10	CALHOUN et al.	
	194	20070109983	A	2007-05-17	Shankar, Rohit et al.	
	195	20070111740	A1	2007-05-17	Wandel	
	196	20070124077	A1	2007-05-31	Hedlund	
	197	20070130283	A1	2007-06-07	Klein et al.	
	198	20070130315	A1	2007-06-07	Friend et al.	
	199	20070140113	A1	2007-06-21	Germelos	
	200	20070140145	A	2007-06-21	Kumar et al.	
	201	20070140275		2007-06-21	BOWMAN et al.	
	202	20070143824	A1	2007-06-21	Shahbazi, Majid	
	203	20070147317	A	2007-06-28	Smith et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	204	20070147324		2007-06-28	McGary, Faith	
	205	20070155365	A	2007-07-05	Kim, Sung-Jun et al.	
	206	20070165630	A1	2007-07-19	Rasanen et al.	
	207	20070168499	A	2007-07-19	Chu, Jing-Long	
	208	20070171856	A1	2007-07-26	Bruce et al.	
	209	20070174490	A1	2007-07-26	Choi et al.	
	210	20070191006	A1	2007-08-16	Carpenter	
	211	20070192460	A1	2007-08-16	Choi et al.	
	212	20070198656		2007-08-23	MAZZAFERRI et al.	
	213	20070201502	A1	2007-08-30	Abramson, Nathan	
	214	20070213054	A1	2007-09-13	Han, Seung-Wook	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

215	20070220251		2007-09-20	ROSENBERG et al.	
216	20070226225		2007-09-27	YIU et al.	
217	20070226775	A	2007-09-27	Andreasen et al.	
218	20070234402	A1	2007-10-04	Khosravi et al.	
219	20070242659	A1	2007-10-18	Cantu et al.	
220	20070243862		2007-10-18	COSKUN et al.	
221	20070248100	A1	2007-10-25	Zuberi et al.	
222	20070254646	A1	2007-11-01	Sokondar	
223	20070254675		2007-11-01	ZORLU OZER et al.	
224	20070255769	A1	2007-11-01	Agrawal et al.	
225	20070255797	A1	2007-11-01	Dunn et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	226	20070255848		2007-11-01	SEWALL et al.	
	227	20070257767	A1	2007-11-08	Beeson, Curt	
	228	20070259656	A	2007-11-08	Jeong, Jong Woo	
	229	20070259673		2007-11-08	WILLARS et al.	
	230	20070263558		2007-11-15	SALOMONE, Leonardo	
	231	20070266422	A1	2007-11-15	Germano et al.	
	232	20070274327		2007-11-29	KAARELA et al.	
	233	20070280453		2007-12-06	Kelley, Sean S.	
	234	20070282896		2007-12-06	WYDROUG et al.	
	235	20070293191	A1	2007-12-20	Mir et al.	
	236	20070294395		2007-12-20	STRUB et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

237	20070294410	A1	2007-12-20	Pandya et al.	
238	20070297378	A1	2007-12-27	Poyhonen et al.	
239	20070298764		2007-12-27	CLAYTON, Steve	
240	20070299965	A1	2007-12-27	Nieh et al.	
241	20070300252		2007-12-27	Acharya, Swarup et al.	
242	20080005285		2008-01-03	ROBINSON et al.	
243	20080005561		2008-01-03	BROWN et al.	
244	20080010379	A	2008-01-10	Zhao, Hang	
245	20080010452		2008-01-10	HOLTZMAN et al.	
246	20080018494	A1	2008-01-24	Waite et al.	
247	20080022354	A	2008-01-24	Grewal, Karanvir et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

248	20080025230	A	2008-01-31	Patel et al.	
249	20080032715	A1	2008-02-07	Jia et al.	
250	20080034063	A1	2008-02-07	Yee, Robert	
251	20080034419	A	2008-02-07	Mullick et al.	
252	20080039102		2008-02-14	SEWALL et al.	
253	20080049630		2008-02-28	KOZISEK et al.	
254	20080050715	A1	2008-02-28	Golczewski et al.	
255	20080051076		2008-02-28	O'Shaughnessy, John et al.	
256	20080052387		2008-02-28	HEINZ et al.	
257	20080056273	A	2008-03-06	Pelletier et al.	
258	20080059474		2008-03-06	LIM, Keng	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

259	20080059743		2008-03-06	BYCHKOV et al.	
260	20080060066		2008-03-06	WYNN et al.	
261	20080062900		2008-03-13	RAO, Bindu Rama	
262	20080064367		2008-03-13	NATH et al.	
263	20080066149		2008-03-13	LIM, Keng	
264	20080066150		2008-03-13	LIM, Keng	
265	20080066181	A1	2008-03-13	Haveson et al.	
266	20080070550	A	2008-03-20	Hose, David Alan	
267	20080077705	A1	2008-03-27	Li et al.	
268	20080080457	A1	2008-04-03	Cole, Terry L.	
269	20080081606		2008-04-03	COLE, Terry L.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

270	20080082643		2008-04-03	STORRIE et al.	
271	20080083013		2008-04-03	SOLIMAN et al.	
272	20080085707		2008-04-10	FADELL, Tony	
273	20080089295	A	2008-04-17	Keeler, James D. et al.	
274	20080089303	A1	2008-04-17	Wirtanen et al.	
275	20080095339		2008-04-24	ELLIOTT et al.	
276	20080096559	A1	2008-04-24	Phillips et al.	
277	20080098062		2008-04-24	BALIA, Hinal K.	
278	20080109679		2008-05-08	WRIGHT et al.	
279	20080120129	A	2008-05-22	Seubert et al.	
280	20080120668		2008-05-22	Yau, Frank Chuen-Foo	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	281	20080120688		2008-05-22	QIU et al.	
	282	20080125079	A1	2008-05-29	O'Neil et al.	
	283	20080126287	A1	2008-05-29	Cox et al.	
	284	20080127304	A1	2008-05-29	Ginter et al.	
	285	20080130534		2008-06-05	TOMIOKA, Tazuko	
	286	20080130656		2008-06-05	KIM et al.	
	287	20080132201		2008-06-05	KARLBERG, Johan	
	288	20080132268	A1	2008-06-05	Choi-Grogan et al.	
	289	20080134330		2008-06-05	KAPOOR et al.	
	290	20080139210	A	2008-06-12	Gisby et al.	
	291	20080147454		2008-06-19	WALKER et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

292	20080160958		2008-07-03	ABICHANDANI et al.	
293	20080162637		2008-07-03	ADAMCZYK et al.	
294	20080162704		2008-07-03	POPLETT et al.	
295	20080164304		2008-07-10	NARASIMHAN et al.	
296	20080166993	A1	2008-07-10	Gautier et al.	
297	20080167027		2008-07-10	GAUTIER et al.	
298	20080167033		2008-07-10	BECKERS, Michel	
299	20080168275	A1	2008-07-10	DeAtley et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

2	101035308	CN	A	2006-03-09	Huawei Tech. Co. Ltd.	☐
3	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.	☐
4	101115248	CN	A	2008-01-30	Lenovo Beijing Ltd.	☐
5	101123553	CN	A	2007-09-11	SouTheast University	☐
6	101127988	CN	A	2008-02-20	ZTE Corporation	☐
7	101155343	CN	B	2006-09-29	Huawei Tech. Co. Ltd.	☐
8	101183958	CN	A	2008-05-21	Huawei Tech. Co. Ltd.	☐
9	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.	☐
10	101341764	CN	A	2009-01-07	Telefonaktiebolaget LM Ericsson	☐
11	101815275	CN	A	2010-08-25	Yang, Liu	☐
12	1310401	CN	A	2001-08-29	Wang, Di Xing	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

13	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.	☐
14	1508734	CN	A	2004-06-30	Chinese Creative Corp.	☐
15	1538730	CN	A	2004-10-20	Zhongxing Communication Co., Ltd.	☐
16	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.	☐
17	1801829	CN	A	2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.	☐
18	1802839	CN	A	2006-07-12	Motorola Inc.	☐
19	1867024	CN	A	2006-11-22	Huawei Technologies Co., Ltd.	☐
20	1878160	CN	A	2006-12-13	Huawei Technologies Co., Ltd.	☐
21	1889777	CN	A	2006-07-19	Huawei Tech. Co. Ltd.	☐
22	1937511	CN	A	2007-03-28	ZTE	☐
23	1098490	EP	A2	2001-05-09	Nortel Networks Ltd.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	24	1289326	EP	A1	2003-03-05	Motorola, Inc.		☐
	25	1463238	EP		2004-09-29	Alcatel		☐
	26	1503548	EP	A1	2005-02-02	FG Microtec GmbH		☐
	27	1545114	EP	A1	2005-06-22	Alcatel		☐
	28	1739518	EP		2007-01-03	Research In Motion Limited		☐
	29	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		☐
	30	1850575	EP	A1	2007-10-31	Research In Motion		☐
	31	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		☐
	32	1942698	EP	A1	2008-07-09	Apple Inc.		☐
	33	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		☐
	34	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	35	2026514	EP	A1	2009-02-18	Nokia Siemens Networks		☐
	36	2005339247	JP	A	2005-12-08	Secured Communications		☐
	37	2006041989	JP		2006-02-09	Fujitsu Ltd.		☐
	38	2006155263	JP	A	2006-06-15	NEC Corporation		☐
	39	2006197137	JP		2006-07-27	NTT Docomo Inc.		☐
	40	2006344007	JP	A	2006-12-21	Hitachi Ltd.		☐
	41	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.		☐
	42	2008301121	JP	A	2008-12-11	Kyocera Corp.		☐
	43	2009111919	JP		2009-05-21	Kyocera Communications Systems		☐
	44	2009212707	JP	A	2009-09-17	Fujitsu Ltd.		☐
	45	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	46	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	47	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	48	20040053858	KR	A	2004-06-25	Electronics and Telecommunications Research Instit		☐
	49	0208863	WO		2002-01-31	Telemac Corp.		☐
	50	1998058505	WO		1998-12-23	Sonera Oy		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐
	4	"End to End QoS Solution for Real-time Multimedia Application," Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

5	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
6	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
7	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
8	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
9	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
10	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
11	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
12	Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009	☐
13	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003; Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WiSPr)	☐
14	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	☐
15	BYRD, "Open Secure Wireless," May 5, 2010	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

16	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 26, 2008	☐
17	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐
18	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
19	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	☐
20	DIKAIKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
21	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐
22	Droid Wall 1.3.7 description 20100428 obtained from https://www.freewarelovers.com/android/apps/droid-wall	☐
23	Ehnert, "Small application to monitor IP traffic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	☐
24	European Commission, "Data Roaming Tariffs - Transparency Measures," obtained from EUROPA - Europe's Information Society Thematic Portal website, June 24, 2011: " http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm ."	☐
25	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐
26	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

27	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
28	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
29	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
30	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
31	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐
32	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	☐
33	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
34	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
35	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	☐
36	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes in Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
37	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

38	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	☐
39	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐
40	Li, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
41	Loopt User Guide, metroPCS, 7/17/2008	☐
42	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	☐
43	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	☐
44	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
45	Nuzman et al., "A compound model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐
46	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	☐
47	OPPLIGER, Rolf, "Internet Security: Firewalls and Beyond," Communications of the ACM, May 1997, Vol. 40, No. 5	☐
48	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2414	
	Examiner Name	NOT YET ASSIGNED	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

49	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
50	Rivadeneira et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐
If you wish to add additional non-patent literature document citation information please click the Add button		
EXAMINER SIGNATURE		
Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered 03/20/2024
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.		
<small> ¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached. </small>		

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	5131020	A	1992-07-14	Liebesny et al.	
	2	5283904		1994-02-01	CARSON, David G. et al.	
	3	5325532	A	1994-06-28	Crosswy et al.	
	4	5572528	A	1996-11-05	Shuen, Pauline	
	5	5577100	A	1996-11-19	McGregor et al.	
	6	5594777		1997-01-14	Makkonen, Matti et al.	
	7	5617539	A	1997-04-01	Ludwig et al.	
	8	5630159	A	1997-05-13	Zancho, William F.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

9	5633484	A	1997-05-27	Zancho, William F. et al.	
10	5633868	A	1997-05-27	Baldwin et al.	
11	5751719	A	1998-05-12	Chen et al.	
12	5754953	A	1998-05-19	Briancon et al.	
13	5774532	A	1998-06-30	Gottlieb et al.	
14	5794142		1998-08-11	VANTTILA et al.	
15	5814798	A	1998-09-29	Zancho, William F.	
16	5889477		1999-03-30	Fastenrath, Ulrich	
17	5892900		1999-04-06	GINTER et al.	
18	5903845		1999-05-11	BUHRMANN et al.	
19	5915008	A	1999-06-22	Dulman, Scott	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

20	5915226	A	1999-06-22	Martineau	
21	5933778		1999-08-03	BUHRMANN et al.	
22	5940472		1999-08-17	NEWMAN et al.	
23	5974439	A	1999-10-26	Boliella, Gregory	
24	5983270	A	1999-11-09	Abraham et al.	
25	6035281		2000-03-07	Crosskey, James P. et al.	
26	6038452		2000-03-14	Strawczynski, Leo et al.	
27	6038540	A	2000-03-14	Krist et al.	
28	6047268		2000-04-04	BARTOLI et al.	
29	6058434	A	2000-05-02	Wilt et al.	
30	6061571	A	2000-05-09	Tamura, Hideo	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

31	6064878		2000-05-16	DENKER, John Stewart et al.	
32	6078953		2000-06-20	VAID et al.	
33	6081591		2000-06-27	SKOOG, Frederick H.	
34	6098878		2000-08-08	DENT et al.	
35	6104700	A	2000-08-15	Haddock, Stephen R. et al.	
36	6115823	A	2000-09-05	Velasco et al.	
37	6119933	A	2000-09-19	Wong et al.	
38	6125391	A	2000-09-26	Meltzer et al.	
39	6141565	A	2000-10-31	Feuerstein et al.	
40	6141686		2000-10-31	JACKOWSKI et al.	
41	6148336		2000-11-14	THOMAS et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	6154738		2000-11-28	CALL, Charles Gainor	
43	6157636	A	2000-12-05	Voit et al.	
44	6185576	B1	2001-02-06	Mcintosh, Lowrie	
45	6198915		2001-03-06	McGREGOR et al.	
46	6219786	B1	2001-04-17	Cunningham et al.	
47	6226277		2001-05-01	Chuah, Mooi Choo	
48	6246870	B1	2001-06-12	Dent et al.	
49	6263055		2001-07-17	GARLAND et al.	
50	6292828		2001-09-18	Williams, David L.	
51	6317584		2001-11-13	ABU-AMARA et al.	
52	6370139	B2	2002-04-09	Redmond	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	6381316		2002-04-30	JOYCE, Simon James et al.	
54	6393014	B1	2002-05-21	Daly et al.	
55	6397259	B1	2002-05-28	Lincke et al.	
56	6401113	B2	2002-06-04	Lazaridis et al.	
57	6418147		2002-07-09	WIEDEMAN, Robert A.	
58	6438575	B1	2002-08-20	Khan et al.	
59	6445777	B1	2002-09-03	Clark, Curtis	
60	6449479		2002-09-10	SANCHEZ, Eduardo	
61	6466984	B1	2002-10-15	Naveh et al.	
62	6477670		2002-11-05	Ahmadvand, Nima	
63	6502131		2002-12-31	VAID, Aseem et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

64	6505114		2003-01-07	LUCIANI, Sergio	
65	6510152	B1	2003-01-21	Gerszberg et al.	
66	6522629	B1	2003-02-18	Anderson, Sr., Ronald D.	
67	6532235		2003-03-11	BENSON et al.	
68	6532579		2003-03-11	SATO et al.	
69	6535855	B1	2003-03-18	Cahill et al.	
70	6535949	B1	2003-03-18	Parker, Kenneth W.	
71	6539082		2003-03-25	LOWE et al.	
72	6542500	B1	2003-04-01	Gerszberg et al.	
73	6542992		2003-04-01	Peirce, Kenneth L. et al.	
74	6546016	B1	2003-04-08	Gerszberg et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

75	6563806		2003-05-13	YANO et al.	
76	6570974	B1	2003-05-27	Gerszberg et al.	
77	6574321		2003-06-03	COX et al.	
78	6574465		2003-06-03	MARSH et al.	
79	6578076	B1	2003-06-10	Putzolu, David Matthew	
80	6581092		2003-06-17	MOTOYAMA, Tetsuro	
81	6591098	B1	2003-07-08	Shieh et al.	
82	6598034	B1	2003-07-22	Kloth, Axel K.	
83	6601040	B1	2003-07-29	Kolis, H. Brock	
84	6603969		2003-08-05	VUORISTO et al.	
85	6603975	B1	2003-08-05	Inouchi et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

86	6606744		2003-08-12	MIKURAK, Michael G.	
87	6628934	A	2003-09-30	Rosenberg et al.	
88	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
89	6636721	B2	2003-10-21	Threadgill et al.	
90	6639975	B1	2003-10-28	O'Neal et al.	
91	6640097		2003-10-28	Corrigan, Louis et al.	
92	6640334	B	2003-10-28	Rasmussen, John H.	
93	6650887		2003-11-18	McGREGOR et al.	
94	6651101		2003-11-18	GAI et al.	
95	6654786	B1	2003-11-25	Fox et al.	
96	6654814		2003-11-25	Britton, Kathryn H. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2414	
	Examiner Name	NOT YET ASSIGNED	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	97	6658254		2003-12-02	PURDY et al.	
	98	6662014	B1	2003-12-09	Walsh, Patrick Jay	
	99	6678516	B2	2004-01-13	Nordman et al.	
	100	6683853		2004-01-27	Kannas, Chris et al.	
	101	6684244		2004-01-27	GOLDMAN et al.	
	102	6690918	B2	2004-02-10	Evans et al.	
	103	6697821	B2	2004-02-24	Ziff et al.	
	104	6725031		2004-04-20	WATLER et al.	
	105	6725256	B1	2004-04-20	Alibal et al.	
	106	6732176	B1	2004-05-04	Stewart et al.	
	107	6735206	B1	2004-05-11	Oki et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	108	6748195	B1	2004-06-08	Phillips, W. Garland	
	109	6748437	B1	2004-06-08	Mankude et al.	
	110	6751296	B1	2004-06-15	Albal et al.	
	111	6754470		2004-06-22	Hendrickson, Keith et al.	
	112	6757717	B1	2004-06-29	Goldstein, Leonid	
	113	6760417	B1	2004-07-06	Wallenius, Jukka	
	114	6763000		2004-07-13	WALSH, Peter J.	
	115	6763226	B1	2004-07-13	McZeal Jr., Alfred	
	116	6765864		2004-07-20	NATARAJAN et al.	
	117	6765925		2004-07-20	Sawyer, Wilson et al.	
	118	6782412		2004-08-24	BROPHY, Kevin et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	119	6785889		2004-08-31	WILLIAMS, Peter	
	120	6792461	B1	2004-09-14	Hericourt, Olivier	
	121	6829596		2004-12-07	FRAZEE, Steve	
	122	6829696		2004-12-07	BALMER et al.	
	123	6839340		2005-01-04	Voit, Eric A. et al.	
	124	6842628	B1	2005-01-11	Arnold et al.	
	125	6873988	B2	2005-03-29	Herrmann et al.	
	126	6876653		2005-04-05	AMBE, Shekhar et al.	
	127	6879825	B1	2005-04-12	Daly, Brian Kevin	
	128	6882718	B1	2005-04-19	Smith, Benjamin V.	
	129	6885997	B1	2005-04-26	Roberts, David T.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

130	6901440	B1	2005-05-31	Bimm et al.	
131	6920455		2005-07-19	WESCHLER, Paul	
132	6922562		2005-07-26	Ward, Stephen L. et al.	
133	6928280		2005-08-09	Xanthos, James et al.	
134	6934249	B1	2005-08-23	Bertin, Olivier et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20080168523		2008-07-10	ANSARI et al.	
	2	20080177998		2008-07-24	APSANGI et al.	
	3	20080178300	A1	2008-07-24	Brown et al.	
	4	20080183811	A1	2008-07-31	Kotras et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

5	20080183812		2008-07-31	PAUL et al.	
6	20080184127		2008-07-31	RAFEY et al.	
7	20080189760		2008-08-07	ROSENBERG et al.	
8	20080201266	A	2008-08-21	Chua et al.	
9	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
10	20080212470		2008-09-04	CASTANEDA et al.	
11	20080212751	A1	2008-09-04	Chung, Simon	
12	20080219268		2008-09-11	DENNISON, Larry R.	
13	20080221951		2008-09-11	STANFORTH et al.	
14	20080222692		2008-09-11	ANDERSSON et al.	
15	20080225748		2008-09-18	KHEMANI et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

16	20080229385		2008-09-18	FEDER et al.	
17	20080229388		2008-09-18	MAES, Stephane H.	
18	20080235511		2008-09-25	O'BRIEN, William G. et al.	
19	20080240373		2008-10-02	WILHELM, Robert D.	
20	20080250053	A	2008-10-09	Aaltonen, Janne et al.	
21	20080256593		2008-10-16	VINBERG et al.	
22	20080259924	A1	2008-10-23	Gooch et al.	
23	20080262798		2008-10-23	KIM, Eun Ah et al.	
24	20080263348	A	2008-10-23	Zaltsman et al.	
25	20080268813		2008-10-30	MAES, Stephane H.	
26	20080270212	A	2008-10-30	Blight et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

27	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
28	20080282319	A1	2008-11-13	Fontijn et al.	
29	20080293395	A1	2008-11-27	Mathews et al.	
30	20080298230		2008-12-04	LUFT et al.	
31	20080305793		2008-12-11	GALLAGHER et al.	
32	20080311885		2008-12-18	DAWSON et al.	
33	20080313315	A	2008-12-18	Karaoguz et al.	
34	20080313730		2008-12-18	Iftimie, Sorin et al.	
35	20080316923		2008-12-25	FEDDERS et al.	
36	20080318547		2008-12-25	BALLOU et al.	
37	20080318550		2008-12-25	DeATLEY, Dallas	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

38	20080319879		2008-12-25	CARROLL et al.	
39	20080320497	A1	2008-12-25	Tarkoma et al.	
40	20090005000	A	2009-01-01	Baker, Matthew et al.	
41	20090005005		2009-01-01	FORSTALL et al.	
42	20090006116	A	2009-01-01	Baker, Matthew et al.	
43	20090006200	A	2009-01-01	Baker, Matthew et al.	
44	20090006229	A1	2009-01-01	Sweeney et al.	
45	20090013157		2009-01-08	BEAULE, Stephane	
46	20090016310	A1	2009-01-15	Rasal, Digambar L.	
47	20090036111	A1	2009-02-05	Danford et al.	
48	20090042536	A1	2009-02-12	Bernard et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

49	20090044185	A1	2009-02-12	Krivopaltsev, Eugene	
50	20090046707	A1	2009-02-19	Smires et al.	
51	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
52	20090047989	A1	2009-02-19	Harmon et al.	
53	20090048913	A1	2009-02-19	Shenfield et al.	
54	20090049156	A1	2009-02-19	Aronsson et al.	
55	20090049518	A1	2009-02-19	Roman et al.	
56	20090054030		2009-02-26	GOLDS, David	
57	20090065571	A1	2009-03-12	Jain, Deepak	
58	20090067372		2009-03-12	SHAH, Keyur C. et al.	
59	20090068984		2009-03-12	BURNETT, R. Alan	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

60	20090070379	A1	2009-03-12	Rappaport, Theodore R.	
61	20090077622		2009-03-19	BAUM et al.	
62	20090079699		2009-03-26	SUN, Jian	
63	20090113514		2009-04-30	HU, Q. James	
64	20090125619		2009-05-14	ANTANI, Snehal S.	
65	20090132860	A1	2009-05-21	LIU et al.	
66	20090149154	A1	2009-06-11	Bhasin et al.	
67	20090157792	A1	2009-06-18	Fiatal	
68	20090163173	A1	2009-06-25	Williams, Timothy D.	
69	20090172077		2009-07-02	ROXBURGH, David et al.	
70	20090180391		2009-07-16	PETERSEN et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

71	20090181662	A1	2009-07-16	Fleischman et al.	
72	20090197585		2009-08-06	AARON, Jeffrey A.	
73	20090197612	A1	2009-08-06	Kiiskinen, Arto	
74	20090203352	A1	2009-08-13	Fordon et al.	
75	20090217364	A1	2009-08-27	Salmela et al.	
76	20090219170		2009-09-03	CLARK, Ryan C. et al.	
77	20090248883		2009-10-01	SURYANARAYANA et al.	
78	20090254857	A	2009-10-08	Romine et al.	
79	20090257379		2009-10-15	ROBINSON et al.	
80	20090271514		2009-10-29	THOMAS et al.	
81	20090282127	A	2009-11-12	Leblanc et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	82	20090286507		2009-11-19	O'NEIL et al.	
	83	20090287921		2009-11-19	ZHU et al.	
	84	20090288140	A1	2009-11-19	Huber et al.	
	85	20090291665	A1	2009-11-26	Gaskarth et al.	
	86	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	87	20090307696	A1	2009-12-10	Vais et al.	
	88	20090307746	A1	2009-12-10	DI et al.	
	89	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	90	20090320110	A1	2009-12-24	NICOLSON et al.	
	91	20100017506		2010-01-21	FADELL, Anthony	
	92	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

93	20100027469	A1	2010-02-04	Gurajala et al.	
94	20100027559		2010-02-04	LIN, Hung-Ming et al.	
95	20100030890	A	2010-02-04	Dutta et al.	
96	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
97	20100041365	A1	2010-02-18	Lott et al.	
98	20100042675		2010-02-18	FUJII, Hiroshi	
99	20100043068		2010-02-18	VARADHAN et al.	
100	20100069074	A1	2010-03-18	Kodialam et al.	
101	20100071053		2010-03-18	ANSARI et al.	
102	20100075666	A1	2010-03-25	Garner, Neil Robert	
103	20100077035	A1	2010-03-25	Li et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	104	20100080202		2010-04-01	Hanson, Mark	
	105	20100082431		2010-04-01	RAMER et al.	
	106	20100088387	A1	2010-04-08	Calamera	
	107	20100103820		2010-04-29	FULLER et al.	
	108	20100113020	A1	2010-05-06	Subramanian et al.	
	109	20100121744	A1	2010-05-13	Beiz et al.	
	110	20100131584		2010-05-27	Johnson, William J.	
	111	20100142478	A1	2010-06-10	Forssell et al.	
	112	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	113	20100151866	A1	2010-06-17	Karpov et al.	
	114	20100153781		2010-06-17	HANNA, Stephen R.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

115	20100167696	A	2010-07-01	Smith, Christopher David et al.	
116	20100188975		2010-07-29	RALEIGH, Gregory G.	
117	20100188990		2010-07-29	RALEIGH, Gregory G.	
118	20100188992		2010-07-29	RALEIGH, Gregory G.	
119	20100188994		2010-07-29	RALEIGH, Gregory G.	
120	20100190469	A1	2010-07-29	Vanderveen et al.	
121	20100191576		2010-07-29	RALEIGH, Gregory G.	
122	20100191612		2010-07-29	RALEIGH, Gregory G.	
123	20100191646		2010-07-29	RALEIGH, Gregory G.	
124	20100192170		2010-07-29	RALEIGH, Gregory G.	
125	20100192212		2010-07-29	RALEIGH, Gregory G.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

126	20100195503		2010-08-05	RALEIGH, Gregory G.	
127	20100197268		2010-08-05	RALEIGH, Gregory G.	
128	20100198698		2010-08-05	RALEIGH et al.	
129	20100198939		2010-08-05	RALEIGH, Gregory G.	
130	20100241544		2010-09-23	Benson, Dan et al.	
131	20100248719	A1	2010-09-30	Scholaert, Hugh	
132	20100284327	A	2010-11-11	Miklos, Gyorgy	
133	20100284388	A1	2010-11-11	Fantini et al.	
134	20100287599	A1	2010-11-11	He et al.	
135	20100325420		2010-12-23	KANEKAR, Tushar	
136	20110004917	A1	2011-01-06	Saisa et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

137	20110013569	A	2011-01-20	Scherzer, Shimon et al.	
138	20110019574	A	2011-01-27	Malomsoky et al.	
139	20110081881	A	2011-04-07	Baker, Matthew Donald et al.	
140	20110082790	A	2011-04-07	Baker, Matthew Donald et al.	
141	20110110309	A	2011-05-12	Bennett, James D.	
142	20110126141		2011-05-26	KING et al.	
143	20110145920	A1	2011-06-16	Mahaffey et al.	
144	20110159818	A	2011-06-30	Scherzer, Shimon et al.	
145	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
146	20110185202	A1	2011-07-28	Black et al.	
147	20110244837	A1	2011-10-06	MURATA et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	148	20110249668	A1	2011-10-13	Milligan et al.	
	149	20110264923	A	2011-10-27	Kocher et al.	
	150	20120020296	A	2012-01-26	Scherzer, Shimon et al.	
	151	20120144025	A1	2012-06-07	Melander et al.	
	152	20120166364	A1	2012-06-28	Ahmad et al.	
	153	20120196644	A	2012-08-02	Scherzer, Shimon et al.	
	154	20120238287	A	2012-09-20	Scherzer, Shimon	
	155	20130029653	A	2013-01-31	Baker, Matthew Donald et al.	
	156	20130058274	A	2013-03-07	Scherzer, Shimon et al.	
	157	20130065555	A	2013-03-14	Baker, Matthew Donald et al.	
	158	20130072177	A1	2013-03-21	Ross et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

159	20130084835	A	2013-04-04	Scherzer, Shimon et al.	
160	20130144789		2013-06-06	Aaltonen, Janne et al.	
161	20130225151	A1	2013-08-29	King et al.	
162	20130326356	A9	2013-12-05	Zheng et al.	
163	20140073291	A1	2014-03-13	Hildner et al.	
164	20140241342	A1	2014-08-28	Constantinof, Cristian	
165	20150181628	A1	2015-06-25	Haverinen et al.	
166	20200077892	A1	2020-03-12	Tran	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1999027723	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

2	1999065185	WO	A3	2001-05-03	Briscoe et al.	☐
3	2002045315	WO	A2	2002-06-06	Micromuse	☐
4	2002067616	WO	A1	2002-08-29	Sonera Oyj	☐
5	2002093877	WO	A1	2002-11-21	Nokia Corp.	☐
6	2003014891	WO		2003-02-20	The Boeing Company	☐
7	2003017063	WO	A2	2003-02-27	Apogee Networks	☐
8	2003017065	WO	A2	2003-02-27	Apogee Networks	☐
9	2003058880	WO	A1	2003-07-17	Eriksson et al.	☐
10	2004028070	WO	A1	2004-04-01	Mann et al.	☐
11	2004064306	WO	A2	2004-07-29	Wild et al.	☐
12	2004077797	WO	A3	2008-02-07	Erskine et al.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

13	2004095753	WO	A3	2005-01-13	Adwankar et al.	☐
14	2005008995	WO		2005-01-27	Starhub Ltd.	☐
15	2005053335	WO	A1	2005-06-09	Nokia Corp.	☐
16	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.	☐
17	2006004467	WO	A1	2006-01-12	Skog et al.	☐
18	2006004784	WO	A1	2006-01-12	Japan Communications Inc.	☐
19	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.	☐
20	2006050758	WO	A1	2006-05-18	Boman	☐
21	2006073837	WO	A3	2009-04-02	D'agostino, Anthony	☐
22	2006077481	WO	A1	2006-07-27	Chane et al.	☐
23	2006093961	WO	A1	2006-09-08	Kyocera Wireless Corp.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

24	2006120558	WO		2006-11-16	Nokia Corp.	☐
25	2006130960	WO	A1	2006-12-14	Sharif-Ahmadi et al.	☐
26	2007001833	WO	A2	2007-01-04	Linsley-Hood et al.	☐
27	2007014630	WO	A1	2007-02-08	Norrman et al.	☐
28	2007018363	WO	A1	2007-02-15	Son	☐
29	2007053848	WO	A1	2007-05-10	Germano et al.	☐
30	2007068288	WO		2007-06-21	Telefonaktiebolaget LM Ericsson	☐
31	2007069245	WO	A3	2009-04-16	Touboul	☐
32	2007097786	WO	A	2007-08-30	Sony Ericsson Mobile Communications AB	☐
33	2007107701	WO	A2	2007-09-27	Cofta	☐
34	2007120310	WO		2007-10-25	Qualcomm Inc.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

35	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		☐
36	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐
37	2007129180	WO	A2	2007-11-15	Nokia Corp.		☐
38	2007133844	WO	A	2007-11-22	Camiant, Inc.		☐
39	2008017837	WO	A1	2008-02-14	Spooner		☐
40	2008051379	WO	A2	2008-05-02	Balia		☐
41	2008066419	WO	A1	2008-06-05	LIDSTRÖM et al.		☐
42	2008080139	WO	A1	2008-07-03	Pugh et al.		☐
43	2008080430	WO	A1	2008-07-10	Costa et al.		☐
44	2008099802	WO	A1	2008-08-21	Awano		☐
45	2009008817	WO	A1	2009-01-15	Ericsson		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	46	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson		☐
	47	2010088413	WO	A1	2010-08-05	Raleigh		☐
	48	2010128391	WO	A2	2010-11-11	Bridgewater Systems Corp.		☐
	49	2010128391	WO	A3	2011-01-20	Montahan et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	2	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	3	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐
	4	SHARKEY, "Coding for Life--Battery Life, That Is," May 27, 2009	☐
	5	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

6	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐
7	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
8	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐
9	Windows7 Power Management, published April 2009	☐
10	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	03/20/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	6934751	B2	2005-08-23	Jayapalan et al.	
	2	6947723		2005-09-20	Gurnani, Roger et al.	
	3	6947985	B2	2005-09-20	Hegli et al.	
	4	6952428		2005-10-04	NECKA et al.	
	5	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	6	6959202	B2	2005-10-25	Heinonen et al.	
	7	6959393	B2	2005-10-25	Hollis et al.	
	8	6965667		2005-11-15	TRABANDT et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

9	6965872		2005-11-15	Grdina, Jerome M.	
10	6967958		2005-11-22	ONO, Yoshiyuki et al.	
11	6970692	B2	2005-11-29	Tysor, Arthur James	
12	6970927	B1	2005-11-29	Stewart et al.	
13	6982733	B1	2006-01-03	McNaily et al.	
14	6983370	B2	2006-01-03	Eaton et al.	
15	6996062	B1	2006-02-07	Freed et al.	
16	6996076		2006-02-07	FORBES et al.	
17	6996393		2006-02-07	Pyhalammi, Seppo et al.	
18	6998985		2006-02-14	REISMAN et al.	
19	7002920		2006-02-21	Ayyagari, Deepak et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

20	7007295	B1	2006-02-28	Rose et al.	
21	7013469	B2	2006-03-14	Smith et al.	
22	7017189	B1	2006-03-21	DeMello et al.	
23	7024200		2006-04-04	McKENNA et al.	
24	7024460	B2	2006-04-04	Koopmas et al.	
25	7027055	B2	2006-04-11	Anderson et al.	
26	7027408		2006-04-11	NABKEL et al.	
27	7031733	B2	2006-04-18	Aiminana et al.	
28	7032072	B1	2006-04-18	Quinn et al.	
29	7039027	B2	2006-05-02	Bridgelall, Raj	
30	7039037		2006-05-02	Wang, Jiwei R. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

31	7039403		2006-05-02	Wong, Gregory A.	
32	7039713	B1	2006-05-02	Van Gunter, David et al.	
33	7042988		2006-05-09	JUITT et al.	
34	7043225	B1	2006-05-09	Patel et al.	
35	7043226		2006-05-09	Yamauchi, Toshiaki	
36	7043268	B2	2006-05-09	Yukie et al.	
37	7047276	B2	2006-05-16	Liu et al.	
38	7058022	B1	2006-06-06	Caroian et al.	
39	7058968		2006-06-06	ROWLAND et al.	
40	7068600		2006-06-27	CAIN, Joseph Bibb	
41	7069248		2006-06-27	HUBER, Adriano	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	7082422	B1	2006-07-25	Zirngibl et al.	
43	7084775	B1	2006-08-01	Smith, Michael R.	
44	7092696		2006-08-15	HOSAIN et al.	
45	7095754	B2	2006-08-22	Benveniste, Mathilde	
46	7102620	B2	2006-09-05	Harries, Andrew Stanely Guy et al.	
47	7110753	B2	2006-09-19	Campen, Kenneth Brian	
48	7113780	B2	2006-09-26	Mckenna Daniel et al.	
49	7113997		2012-09-26	Jayapalan, Jay et al.	
50	7120133	B1	2006-10-10	Joo et al.	
51	7133386	B2	2006-11-07	Holur et al.	
52	7133695	B2	2006-11-07	Beyda, William J.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	7136361	B2	2006-11-14	Benveniste, Mathilde	
54	7139569	B2	2006-11-21	Kato, Akira	
55	7142876		2006-11-28	TROSSEN et al.	
56	7149229	B1	2006-12-12	Leung, Kent K.	
57	7149521	B2	2006-12-12	Sundar et al.	
58	7151764	B1	2006-12-19	Heinonen et al.	
59	7158792		2007-01-02	COOK et al.	
60	7162237	B1	2007-01-09	Silver et al.	
61	7165040	B2	2007-01-16	Ehrman et al.	
62	7167078		2007-01-23	POURCHOT, Shawn C.	
63	7171199	B1	2007-01-30	Rahman	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

64	7174156	B1	2007-02-06	Mangai, Manish	
65	7174174		2007-02-06	BORIS et al.	
66	7177919	B1	2007-02-13	Truong et al.	
67	7180855		2007-02-20	LIN , Wei	
68	7181017		2007-02-20	Nagei, Robert H. et al.	
69	7191248	B2	2007-03-13	Chattopadhyay et al.	
70	7197321		2007-03-27	ERSKINE et al.	
71	7200112	B2	2007-04-03	Sundar et al.	
72	7200551	B1	2007-04-03	Senez	
73	7203169	B1	2007-04-10	Okholm, Jon et al.	
74	7203721	B1	2007-04-10	Ben-Efraim et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

75	7203752	B2	2007-04-10	Rice et al.	
76	7212491		2007-05-01	Koga, Takahiro	
77	7219123	B1	2007-05-15	Fiechter et al.	
78	7222190	B2	2007-05-22	Klinker et al.	
79	7222304	B2	2007-05-22	Beaton et al.	
80	7224968	B2	2007-05-29	Dobson et al.	
81	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
82	7236780		2007-06-26	Benco, David S.	
83	7242668	B2	2007-07-10	Kan et al.	
84	7242920		2007-07-10	MORRIS, Robert P.	
85	7245901		2007-07-17	McGREGOR et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

86	7248570	B2	2007-07-24	Bahl et al.	
87	7248868	B2	2007-07-24	Snyder et al.	
88	7251218		2007-07-31	Jorgensen, Jacob W.	
89	7260382	B1	2007-08-21	Lamb et al.	
90	7266371	B1	2007-09-04	Amin et al.	
91	7269157	B2	2007-09-11	Klinker et al.	
92	7271765	B2	2007-09-18	Stilp et al.	
93	7272660	B1	2007-09-18	Powers et al.	
94	7280816		2007-10-09	FRATTI et al.	
95	7280818		2007-10-09	CLAYTON, Steve	
96	7283561		2007-10-16	Picher-Dempsey, Heidi	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

97	7283963		2007-10-16	FITZPATRICK, John E. et al.	
98	7286834	B2	2007-10-23	Walter	
99	7286848	B2	2007-10-23	Vireday, Richard P. et al.	
100	7289489		2007-10-30	KUNG et al.	
101	7290283		2007-10-30	COPELAND III, John A.	
102	7310424		2007-12-18	Gehring, Stephan Walter et al.	
103	7313237	B2	2007-12-25	Bahl, Paramvir et al.	
104	7315892	B2	2008-01-01	Freimuth et al.	
105	7317699		2008-01-08	GODFREY et al.	
106	7318111	B2	2008-01-08	Zhao, Wen	
107	7320029	B2	2008-01-15	Rinne et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

108	7322044		2008-01-22	HRASTAR, Scott E.	
109	7324447		2008-01-29	MORFORD, Michael Robert	
110	7325037		2008-01-29	LAWSON, Karen L.	
111	7336960		2008-02-26	ZAVALKOVSKY et al.	
112	7340772	B2	2008-03-04	Panasyuk et al.	
113	7346410		2008-03-18	UCHIYAMA, Kenji	
114	7349695		2008-03-25	OOMMEN et al.	
115	7353533	B2	2008-04-01	Wright et al.	
116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
117	7356337		2008-04-08	FLORENCE, Shahar	
118	7366497		2008-04-29	NAGATA, Hideaki	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

119	7366654	B2	2008-04-29	Moore, Robert C.	
120	7369848	B2	2008-05-06	Jiang, Yue Jun	
121	7369856	B2	2008-05-06	Ovadia, Shlomo	
122	7373136		2008-05-13	WATLER et al.	
123	7373179		2008-05-13	Stine, Ted et al.	
124	7379731	B2	2008-05-27	Natsuno et al.	
125	7388950		2008-06-17	ELSEY et al.	
126	7389412	B2	2008-06-17	Sharma et al.	
127	7391724	B2	2008-06-24	Alakoski et al.	
128	7395244	B1	2008-07-01	Kingsford, Bryan	
129	7401338		2008-07-15	BOWEN et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

130	7403763		2008-07-22	MAES, Stephane H.	
131	7409447	B	2008-08-05	Assadzadeh, Alireza	
132	7409569	B2	2008-08-05	Illowsky et al.	
133	7411930	B2	2008-08-12	Montejo et al.	
134	7418253		2008-08-26	KAVANAHA, Alan	
135	7418257		2008-08-26	Kim, Myong-Ju	
136	7421004		2008-09-02	FEHER, Kamilo	
137	7423971	B1	2008-09-09	Mohaban et al.	
138	7428750	B1	2008-09-23	Dunn et al.	
139	7433362	B2	2008-10-07	Mallya et al.	
140	7436816	B2	2008-10-14	Mehta et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

141	7440433	B2	2008-10-21	Rink et al.	
142	7444669	B1	2008-10-28	Bahl, Paramvir et al.	
143	7450591		2008-11-11	KORLING et al.	
144	7450927		2008-11-11	CRESWELL et al.	
145	7454191	B2	2008-11-18	Dawson et al.	
146	7457265		2008-11-25	Julka, Vibhor et al.	
147	7457870	B1	2008-11-25	Lownsborough et al.	
148	7460837	B2	2008-12-02	Diener, Neil R.	
149	7466652	B2	2008-12-16	Lau et al.	
150	7467160	B2	2008-12-16	McIntyre	
151	7472189		2008-12-30	Mallya, Arvind R. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

152	7478420	B2	2009-01-13	Wright, Michael et al.	
153	7486185		2009-02-03	CULPEPPER et al.	
154	7486658	B2	2009-02-03	Kumar, Rajneesh	
155	7493659	B1	2009-02-17	Wu, Handong et al.	
156	7496652		2009-02-24	Pezzutti, David	
157	7499438		2009-03-03	Hinman, Brian L. et al.	
158	7499537		2009-03-03	ELSEY et al.	
159	7502672	B1	2009-03-10	Kolis, H. Brock	
160	7505756	B2	2009-03-17	Bahl	
161	7505795	B1	2009-03-17	Lim et al.	
162	7508799	B2	2009-03-24	Sumner et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

163	7512128	B2	2009-03-31	DiMambro et al.	
164	7512131	B2	2009-03-31	Svensson et al.	
165	7515608		2009-04-07	Yuan, Yuan et al.	
166	7515926	B2	2009-04-07	Bu et al.	
167	7516219		2009-04-07	MOGHADDAM et al.	
168	7522549	B2	2009-04-21	Karaoguz et al.	
169	7522576	B2	2009-04-21	Du et al.	
170	7526541	B2	2009-04-28	Roese et al.	
171	7529204	B2	2009-05-05	Bourlas, Yair et al.	
172	7535880		2009-05-19	Hinman, Brian L. et al.	
173	7536695	B2	2009-05-19	Alam et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

174	7539132	B2	2009-05-26	Werner et al.	
175	7539862	B2	2009-05-26	Edgett et al.	
176	7540408	B2	2009-06-02	Levine et al.	
177	7545782		2009-06-09	Rayment, Stephen G. et al.	
178	7546460		2009-06-09	Maes, Stephane H.	
179	7546629		2009-06-09	ALBERT, Anthony et al.	
180	7548875	B2	2009-06-16	Mikkelsen et al.	
181	7548976	B2	2009-06-16	Bahl, Paramvir et al.	
182	7551921	B2	2009-06-23	Petermann	
183	7551922		2009-06-23	Roskowski, Steve et al.	
184	7554983	B1	2009-06-30	Muppala, Suresh	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

185	7555757	B2	2009-06-30	Smith et al.	
186	7561899	B2	2009-07-14	Lee, Changseok	
187	7562213	B1	2009-07-14	Timms, Natalie	
188	7564799	B2	2009-07-21	Holland et al.	
189	7565141		2009-07-21	Macaluso, Anthony G.	
190	7574509	B2	2009-08-11	Nixon et al.	
191	7574731		2009-08-11	FASCENDA, Anthony C.	
192	7577431	B2	2009-08-18	Jiang, Yue Jun	
193	7580356	B1	2009-08-25	Mishra et al.	
194	7580857		2009-08-25	VanFLEET et al.	
195	7583964	B2	2009-09-01	Wong, Gregory A.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

196	7584298	B2	2009-09-01	Klinker et al.	
197	7586871	B2	2009-09-08	Hamilton et al.	
198	7593417		2009-09-22	Wang, James et al.	
199	7593730	B2	2009-09-22	Khandelwal, Deepak et al.	
200	7596373	B2	2009-09-29	Mcgregor, Christopher et al.	
201	7599288		2009-10-06	COLE, Raymond E. et al.	
202	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	
203	7602746	B2	2009-10-13	Calhoun et al.	
204	7606918	B2	2009-10-20	Holzman et al.	
205	7607041	B2	2009-10-20	Kraemer et al.	
206	7609650		2009-10-27	ROSKOWSKI, Steve et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

207	7609700		2009-10-27	Ying, Wen-Ping et al.	
208	7610047	B2	2009-10-27	Hicks III et al.	
209	7610057	B2	2009-10-27	Bahl et al.	
210	7610328		2009-10-27	HAASE et al.	
211	7610396	B2	2009-10-27	Taglienti et al.	
212	7614051	B	2009-11-03	Glaum et al.	
213	7616962	B2	2009-11-10	Oswal, Anand K. et al.	
214	7617516		2009-11-10	HUSLAK et al.	
215	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
216	7620065		2009-11-17	FALARDEAU, Eric	
217	7620162		2009-11-17	AARON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	218	7620383	B2	2009-11-17	Taglienti et al.	
	219	7627314		2009-12-01	Carlson, Steven I. et al.	
	220	7627600	B2	2009-12-01	Citron et al.	
	221	7627767	B2	2009-12-01	Sherman et al.	
	222	7627872	B2	2009-12-01	Hebeleier et al.	
	223	7633438		2009-12-15	Tysowski, Piotr Konrad	
	224	7634388		2009-12-15	Archer, Charles J. et al.	Entire Document
	225	7636574		2009-12-22	Poosala, Viswanath	
	226	7636626	B2	2009-12-22	Oesterling et al.	
	227	7643411	B2	2010-01-05	Andreasen et al.	
	228	7644151		2010-01-05	JERRIM, John et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

229	7644267		2010-01-05	YLIKOSKI, Martti et al.	
230	7644414	B2	2010-01-05	Smith et al.	
231	7647047		2010-01-12	MOGHADDAM et al.	
232	7650137		2010-01-19	JOBS et al.	
233	7653394	B2	2010-01-26	McMillin, Brian K.	
234	7656271	B2	2010-02-02	Ehrman et al.	
235	7657920	B2	2010-02-02	Arseneau et al.	
236	7660419	B1	2010-02-09	Ho, Jin-Meng	
237	7661124	B2	2010-02-09	Ramanathan et al.	
238	7664494	B2	2010-02-16	Jiang, Yue Jun	
239	7668176		2010-02-23	Chuah, Mooi Choo	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

240	7668612	B	2010-02-23	Okkonen, Harri	
241	7668903		2010-02-23	EDWARDS et al.	
242	7668966	B2	2010-02-23	Klinker et al.	
243	7676673	B2	2010-03-09	Weller et al.	
244	7680086	B2	2010-03-16	Eglin	
245	7681226	B2	2010-03-16	Kraemer et al.	
246	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
247	7685131		2010-03-23	Batra, Vishal Singh et al.	
248	7685254		2010-03-23	Pandya, Ashish A.	
249	7685530	B2	2010-03-23	Sherrard et al.	
250	7688792	B2	2010-03-30	Babbar et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

251	7693107	B2	2010-04-06	De Froment, Eric	
252	7693720		2010-04-06	KENNEWICK et al.	
253	7697540	B2	2010-04-13	Haddad et al.	
254	7707320	B2	2010-04-27	Singhai et al.	
255	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	
256	7711848		2010-05-04	MAES, Stephane H.	
257	7719966	B2	2010-05-18	Luft et al.	
258	7720206	B2	2010-05-18	Devolites et al.	
259	7720464	B2	2010-05-18	Batta, Puneet	
260	7720505		2010-05-18	GOPI et al.	
261	7720960	B2	2010-05-18	Pruss, Richard Manfred et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

262	7721296	B2	2010-05-18	Ricagni, Giuseppe	
263	7724716	B2	2010-05-25	Fadell, Anthony M.	
264	7725570		2010-05-25	Lewis, Lundy	
265	7729326		2010-06-01	Sekhar, Ramesh	
266	7730123		2010-06-01	ERICKSON, Richard R. et al.	
267	7734784		2010-06-08	ARAUJO et al.	
268	7742406	B1	2010-06-22	Muppala, Suresh	
269	7746854		2010-06-29	AMBE, Shekhar et al.	
270	7747240		2010-06-29	BRISCOE et al.	
271	7747699		2010-06-29	PRUEITT et al.	
272	7747730		2010-06-29	HARLOW, James D.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

273	7752330	B2	2010-07-06	Olsen et al.	
274	7756056	B2	2010-07-13	Kim et al.	
275	7756534		2010-07-13	Anupam, Vinod et al.	
276	7756757	B1	2010-07-13	Oakes III, Charles Lee	
277	7760137	B2	2010-07-20	Martucci et al.	
278	7760711	B1	2010-07-20	Kung et al.	
279	7760861		2010-07-20	Croak, Marian et al.	
280	7765294	B2	2010-07-27	Edwards et al.	
281	7769397	B2	2010-08-03	Funato et al.	
282	7770785	B2	2010-08-10	Jha et al.	
283	7774323	B2	2010-08-10	Helfman, Nadav	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

284	7774412	B1	2010-08-10	Schnepel, Soenke	
285	7774456	B1	2010-08-10	Lownsborough, Derek Leigh et al.	
286	7778176		2010-08-17	Morford, Michael Robert	
287	7778643		2010-08-17	Laroia, Rajiv et al.	
288	7792257	B1	2010-09-07	Vanier et al.	
289	7792538		2010-09-07	Kozisek, Steven E.	
290	7792708		2010-09-07	ALVA, Jessi	
291	7797019	B2	2010-09-14	Friedmann	
292	7797060	B2	2010-09-14	Grgic et al.	
293	7797204		2010-09-14	BALENT, Bruce F.	
294	7797401		2010-09-14	STEWART et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

295	7801523		2010-09-21	Kenderov, Stoyan	
296	7801783	B2	2010-09-21	Kende et al.	
297	7801985	B1	2010-09-21	Pitkow, Jim et al.	
298	7802724		2010-09-28	Nohr, Steven Paul	
299	7805140	B2	2010-09-28	Friday et al.	
300	7805522	B2	2010-09-28	Schlüter et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2414	
	Examiner Name	NOT YET ASSIGNED	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	1							☐
--	---	--	--	--	--	--	--	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	03/20/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	7805606	B2	2010-09-28	Birger et al.	
	2	7809351	B1	2010-10-05	Panda et al.	
	3	7809372	B2	2010-10-05	Rajaniemi, Jaakko	
	4	7813746	B2	2010-10-12	Rajkotia, Purva R.	
	5	7817615	B1	2010-10-19	Breau et al.	
	6	7817983	B2	2010-10-19	Cassett et al.	
	7	7822837		2010-10-26	URBAN et al.	
	8	7822849	B2	2010-10-26	Titus	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

9	7826427	B2	2010-11-02	Sood et al.	
10	7826607	B1	2010-11-02	De Carvalho Resende et al.	
11	7835275	B1	2010-11-16	Swan et al.	
12	7843831	B2	2010-11-30	Morrill et al.	
13	7843843	B1	2010-11-30	Papp III et al.	
14	7844034	B1	2010-11-30	Oh et al.	
15	7844728	B2	2010-11-30	Anderson et al.	
16	7848768		2010-12-07	OMORI et al.	
17	7849161	B2	2010-12-07	Koch et al.	
18	7849170	B1	2010-12-07	Hargens et al.	
19	7849477	B2	2010-12-07	Cristofalo et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

20	7853255	B2	2010-12-14	Karaoguz et al.	
21	7853656	B2	2010-12-14	Yach et al.	
22	7856226		2010-12-21	WONG, Ellis L. et al.	
23	7860088	B2	2010-12-28	Lioy, Marcello	
24	7865182		2011-01-04	Macaluso, Anthony G.	
25	7865187	B2	2011-01-04	Ramer et al.	
26	7868778		2011-01-11	KENWRIGHT, David Norris	
27	7873001	B2	2011-01-18	Silver, Andrew	
28	7873344		2011-01-18	BOWSER, Robert et al.	
29	7873346	B2	2011-01-18	Petersson et al.	
30	7873540	B2	2011-01-18	Arumugam, Avin	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

31	7873705		2011-01-18	KALISH, Dan	
32	7877090		2011-01-25	Maes, Stephane H.	
33	7881199		2011-02-01	KRSTULICH, Zlatko	
34	7881697	B2	2011-02-01	Baker, Matthew Donald et al.	
35	7882029		2011-02-01	WHITE, Craig R.	
36	7882247	B2	2011-02-01	Stumolo et al.	
37	7882560	B2	2011-02-01	Kraemer et al.	
38	7885644	B2	2011-02-08	Gallagher et al.	
39	7886047		2011-02-08	POTLURI, Dora	
40	7889384	B2	2011-02-15	Armentrout et al.	
41	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	7890111		2011-02-15	Bugenhagen, Michael K.	
43	7894431	B2	2011-02-22	Goring et al.	
44	7899039	B2	2011-03-01	Andreasen et al.	
45	7899438	B2	2011-03-01	Baker, Matthew Donald et al.	
46	7903553		2011-03-08	Liu, Enhui	
47	7907970		2011-03-15	Park, Vincent D. et al.	
48	7911975		2011-03-22	DROZ, Patrick et al.	
49	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
50	7912056		2011-03-22	BRASSEM, Wayne	
51	7920529		2011-04-05	MAHLER, Roger et al.	
52	7921463		2011-04-05	Sood, Kapil et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	7925740	B2	2011-04-12	Nath et al.	
54	7925778	B1	2011-04-12	Wijnands et al.	
55	7929446	B2	2011-04-19	Bozarth et al.	
56	7929959	B2	2011-04-19	DeAtley, Dallas et al.	
57	7929960		2011-04-19	MARTIN et al.	
58	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
59	7930327	B2	2011-04-19	Craft David et al.	
60	7930446	B2	2011-04-19	Kesselman, Alex et al.	
61	7930553	B2	2011-04-19	Satarasinghe et al.	
62	7933274	B2	2011-04-26	Verma et al.	
63	7936736	B2	2011-05-03	Proctor Jr. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

64	7937069		2011-05-03	RASSAM, Frederic	
65	7937450	B2	2011-05-03	Janik, Craig M.	
66	7940685	B1	2011-05-10	Breslau, Lee et al.	
67	7940751		2011-05-10	Hansen, Christopher J.	
68	7941184		2011-05-10	PRENDERGAST et al.	
69	7944948		2011-05-17	Chow, Albert T. et al.	
70	7945238	B2	2011-05-17	Baker, Matthew Donald et al.	
71	7945240		2011-05-17	KLOCK, Jacqueline et al.	
72	7945945		2011-05-17	Graham, Richard et al.	
73	7948952		2011-05-24	HURTTA, Tuija et al.	
74	7948953	B2	2011-05-24	Melkote, Keerti G. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

75	7948968		2011-05-24	Voit, Eric A. et al.	
76	7949529		2011-05-24	WEIDER et al.	
77	7953808		2011-05-31	SHARP et al.	
78	7953877	B2	2011-05-31	Vemula et al.	
79	7957020		2011-06-07	MINE, Ryuta et al.	
80	7957381	B2	2011-06-07	Clermidy et al.	
81	7957511		2011-06-07	DRUDIS et al.	
82	7958029	B1	2011-06-07	Bobich et al.	
83	7962622		2011-06-14	Friend, John et al.	
84	7965983		2011-06-21	SWAN, Tim et al.	
85	7966405	B2	2011-06-21	Sundaresan et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

86	7969950	B2	2011-06-28	Iyer et al.	
87	7970350		2011-06-28	SHEYNMAN, Arnold	
88	7970426		2011-06-28	Poe, Brian R. et al.	
89	7974624		2011-07-05	Gallagher, Michael D. et al.	
90	7975184		2011-07-05	GOFF et al.	
91	7978627		2011-07-12	TAYLOR, William Scott et al.	
92	7978686	B2	2011-07-12	Goyal et al.	
93	7979069	B2	2011-07-12	Hupp et al.	
94	7979889	B2	2011-07-12	Gladstone et al.	
95	7979896	B2	2011-07-12	McMurtry et al.	
96	7984130		2011-07-19	BOGINENI et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

97	7984511	B2	2011-07-19	Kocher Paul et al.	
98	7986935		2011-07-26	D'SOUZA et al.	
99	7987496	B2	2011-07-26	Bryce et al.	
100	7987510	B2	2011-07-26	Kocher et al.	
101	7990049	B2	2011-08-02	Shioya, Shunsuke	
102	8000276	B2	2011-08-16	Scherzer, Shimon et al.	
103	8000318		2011-08-16	Wiley, William L. et al.	
104	8005009		2011-08-23	McKee, Neil et al.	
105	8005459		2011-08-23	BALSILLIE, Jim	
106	8005726	B1	2011-08-23	Bao, Yulin	
107	8005913	B1	2011-08-23	Carlander, Carrie	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

108	8005988		2011-08-23	MAES, Stephane H.	
109	8010080		2011-08-30	THENTHIRUPERAI et al.	
110	8010081		2011-08-30	ROSKOWSKI, Steve	
111	8010082	B2	2011-08-30	Sutaria et al.	
112	8010990	B2	2011-08-30	Ferguson et al.	
113	8015133		2011-09-06	WU et al.	
114	8015234		2011-09-06	LUM et al.	
115	8015249	B2	2011-09-06	Nayak et al.	
116	8019687		2011-09-13	WANG et al.	
117	8019820		2011-09-13	Son, Giyeong et al.	
118	8019846	B2	2011-09-13	Roelens et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

119	8019868		2011-09-13	RAO, Goutham et al.	
120	8023425	B2	2011-09-20	Raleigh	
121	8024397		2011-09-20	ERICKSON, Richard R. et al.	
122	8024424	B2	2011-09-20	Freimuth et al.	
123	8027339	B2	2011-09-27	Short, Joel E. et al.	
124	8031601	B2	2011-10-04	Feroz et al.	
125	8032168	B2	2011-10-04	Ikaheimo, Jorma	
126	8032409	B1	2011-10-04	Mikurak	
127	8032899	B2	2011-10-04	Archer, Charles J. et al.	
128	8036387	B2	2011-10-11	Kudelski et al.	
129	8044792	B2	2011-10-25	Orr et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	130	8045973	B2	2011-10-25	Chambers, Michael D.	
	131	8046449	B2	2011-10-25	Yoshiuchi, Hideya	
	132	8050275		2011-11-01	IYER, Jayaraman R.	
	133	8050690	B2	2011-11-01	Neeraj, Chawla	
	134	8050705	B2	2011-11-01	Sicher et al.	
	135	8059530		2011-11-15	Cole, Terry L.	
	136	8060017	B2	2011-11-15	Schlicht et al.	
	137	8060463		2011-11-15	Spiegel, Joel R.	
	138	8064418	B2	2011-11-22	Maki, Lasse	
	139	8065365	B2	2011-11-22	Saxena et al.	
	140	8068824		2011-11-29	SHAN, Xueshan et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

141	8068829	B2	2011-11-29	Lemond, Eric et al.	
142	8073427	B2	2011-12-06	Koch et al.	
143	8073721		2011-12-06	Lewis, Lundy	
144	8078140	B2	2011-12-13	Baker, Matthew Donald et al.	
145	8078163	B2	2011-12-13	Lemond, Eric et al.	
146	8085808	B2	2011-12-27	Brusca et al.	
147	8086398	B2	2011-12-27	Sanchez et al.	
148	8086497	B1	2011-12-27	Oakes III, Charles Lee	
149	8086791	B2	2011-12-27	Caulkins, Jason	
150	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
151	8090361	B2	2012-01-03	Hagan, Guy R.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	152	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	153	8091087	B2	2012-01-03	Ali et al.	
	154	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	155	8095112	B2	2012-01-10	Chow, Richard et al.	
	156	8095640	B2	2012-01-10	Guingo et al.	
	157	8095666		2012-01-10	SCHMIDT et al.	
	158	8098579		2012-01-17	Ray, Amar N. et al.	
	159	8099077		2012-01-17	CHOWDHURY et al.	
	160	8099517		2012-01-17	JIA et al.	
	161	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	162	8103285	B2	2012-01-24	Kaihan, Amit	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

163	8104080	B2	2012-01-24	Burns et al.	
164	8107953	B2	2012-01-31	Zimmerman et al.	
165	8108520		2012-01-31	Ruutu, Jussi et al.	
166	8108680	B2	2012-01-31	Murray	
167	8112435	B2	2012-02-07	Epstein et al.	
168	8116223		2012-02-14	TIAN, Dan et al.	
169	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
170	8116781	B2	2012-02-14	Chen, Xixian et al.	
171	8122128		2012-02-21	Burke, II, Robert M. et al.	
172	8122249		2012-02-21	Falk, Rainer et al.	
173	8125897	B2	2012-02-28	Ray et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

174	8126123		2012-02-28	Cai, Yigang et al.	
175	8126396	B2	2012-02-28	Bennett, James D.	
176	8126476	B2	2012-02-28	Vardi, Yosef et al.	
177	8126722		2010-02-28	ROBB, Terence Alan et al.	
178	8130793	B2	2012-03-06	Edwards, Stephen K. et al.	
179	8131256		2012-03-06	MARTTI, Jyrki et al.	
180	8131281	B1	2012-03-06	Hildner et al.	
181	8131840	B1	2012-03-06	Denker, Richard E.	
182	8131858	B2	2012-03-06	Agulnik et al.	
183	8132256	B2	2012-03-06	Bari, Farooq	
184	8134954	B2	2012-03-13	Godfrey, James A. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

185	8135388		2012-03-13	Gailloux, Michael A. et al.	
186	8135392		2012-03-13	MARCELLINO et al.	
187	8135657		2012-03-13	Kapoor, Harsh et al.	
188	8140690	B2	2012-03-20	Ly et al.	
189	8144591		2012-03-27	GHAJ et al.	
190	8145194	B2	2012-03-27	Yoshikawa et al.	
191	8146142	B2	2012-03-27	Lortz et al.	
192	8149748	B2	2012-04-03	Bata et al.	
193	8149823		2012-04-03	Turcan, Diane Brown et al.	
194	8150394	B2	2012-04-03	Bianconi et al.	
195	8150431		2012-04-03	Wolovitz, Lionel et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

196	8151205	B2	2012-04-03	Follmann et al.	
197	8155155		2012-04-10	Chow, Albert T. et al.	
198	8155620		2012-04-10	Wang, Jun et al.	
199	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	
200	8155670		2012-04-10	Fullam, Scott et al.	
201	8156206		2012-04-10	KILEY, Kevin J. et al.	
202	8159520	B1	2012-04-17	Dhanoa et al.	
203	8160056	B2	2012-04-17	Van der Merwe et al.	
204	8160598	B2	2012-04-17	Savoor, Raghvendra	
205	8165576		2012-04-24	Raju, Vishwanath et al.	
206	8166040	B2	2012-04-24	Brindisi, Richard G. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

207	8166554	B2	2012-04-24	John, Pramod	
208	8170553		2012-05-01	BENNETT, James D.	
209	8174378	B2	2012-05-08	Richman et al.	
210	8174970	B2	2012-05-12	Adamczyk, Maria et al.	
211	8175574	B1	2012-05-08	Panda et al.	
212	8180881	B2	2012-05-15	Seo et al.	
213	8180886	B2	2012-05-15	Overcash et al.	
214	8184530		2012-05-22	SWAN, Tim L. et al.	
215	8184590		2012-05-22	Rosenblatt, Ariel	
216	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
217	8185127	B1	2012-05-22	Cai et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

218	8185152		2012-05-22	GOLDNER, Alla	
219	8185158		2012-05-22	Tamura, Motoshi et al.	
220	8190087	B2	2012-05-29	Fisher et al.	
221	8190122	B1	2012-05-29	Alexander et al.	
222	8190675		2012-05-29	TRIBBETT, David	
223	8191106	B2	2012-05-29	Choyi et al.	
224	8191116		2012-05-29	Gazzard, Daryl	
225	8191124	B2	2012-05-29	Wynn et al.	
226	8194549	B2	2012-06-05	Huber et al.	
227	8194553		2012-06-05	LIANG, Zhi Yong et al.	
228	8194581	B1	2012-06-05	Schroeder et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

229	8195153	B1	2012-06-05	Frencel et al.	
230	8195163	B2	2012-06-05	Gisby, Doug et al.	
231	8195661	B2	2012-06-05	Kalavade, Asawaree	
232	8196199	B2	2012-06-05	Hrastar et al.	
233	8200163	B2	2012-06-12	Hoffman, George E.	
234	8200200	B1	2012-06-12	Beiser et al.	
235	8200509	B2	2012-06-12	Kenedy, Andrew Alexander et al.	
236	8200775		2012-06-12	MOORE, James F.	
237	8200818	B2	2012-06-12	Freund et al.	
238	8204190	B2	2012-06-19	Bang et al.	
239	8204505	B2	2012-06-19	Jin et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

240	8208788	B2	2012-06-26	Ando et al.	
241	8208919		2012-06-26	KOTECHEA, Lalit Ratilal	
242	8213296		2012-07-03	SHANNON, Frank M. et al.	
243	8213363		2012-07-03	Ying, Wen-Ping et al.	
244	8214536		2012-07-03	ZHAO, Wen	
245	8214890	B2	2012-07-03	Kirovski et al.	
246	8219134	B2	2012-07-10	Maharajh et al.	
247	8223655	B2	2012-07-17	Heinz et al.	
248	8224382		2012-07-17	Bultman, Michael J.	
249	8224773		2012-07-17	Spiegel, Joel R.	
250	8228818	B2	2012-07-24	Chase et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

251	8229394	B2	2012-07-24	Kariberg, Johan	
252	8229914	B2	2012-07-24	Ramer et al.	
253	8233433	B2	2012-07-31	Kalhan, Amit	
254	8233883		2012-07-31	De Froment, Eric	
255	8233895		2012-07-31	Tysowski, Piotr Konrad	
256	8238287		2012-08-07	Gopi, Paramesh et al.	
257	8239520		2012-08-07	GRAH, Adrian	
258	8242959	B2	2012-08-14	Mia, Rashidus S. et al.	
259	8244241		2012-08-14	Montemurro, Michael	
260	8249601	B2	2012-08-21	Emberson et al.	
261	8254880	B2	2012-08-28	Aaltonen et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	262	8254915		2012-08-28	Kozisek, Steven E.	
	263	8255515		2012-08-28	MELMAN, David et al.	
	264	8255534	B2	2012-08-28	Assadzadeh, Alireza	
	265	8255689		2012-08-28	KIM, Eun Ah et al.	
	266	8259692	B2	2012-09-04	Bajko, Gabor	
	267	8264965	B2	2012-09-11	Dolganow et al.	
	268	8265004		2012-09-11	Toutonghi, Michael J.	
	269	8266249	B2	2012-09-11	Hu	
	270	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	271	8270955	B2	2012-09-18	Ramer et al.	
	272	8270972	B2	2012-09-18	Otting, Marcia J. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

273	8271025	B2	2012-09-18	Brisebois et al.	
274	8271045		2012-09-18	Parolkar, Satish et al.	
275	8271049		2012-09-18	SILVER, Andrew et al.	
276	8271992	B2	2012-09-18	Chatley, Scott P. et al.	
277	8275415	B2	2012-09-25	Huslak, Nicholas S.	
278	8279067		2012-10-02	BERGER, Thomas R. et al.	
279	8279864		2012-10-02	Wood, Daniel M.	
280	8280354		2012-10-02	Smith, Christopher et al.	
281	8284740		2012-10-09	O'CONNOR, Dennis M.	
282	8285249	B2	2012-10-09	Baker, Matthew Donald et al.	
283	8285992	B2	2012-10-09	Mathur et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

284	8291238		2012-10-16	GINTER, Karl L. et al.	
285	8291439	B2	2012-10-16	Jethi et al.	
286	8296404		2012-10-23	McDysan, Dave et al.	
287	8300575	B2	2012-10-30	Willars, Per	
288	8307067	B2	2012-11-06	Ryan, Nicholas M.	
289	8310943	B2	2012-11-13	Mehta et al.	
290	8315198	B2	2012-11-20	Corneille et al.	
291	8315593	B2	2012-11-20	Gallant et al.	
292	8315999	B2	2012-11-20	Chatley, Scott P. et al.	
293	8320244	B2	2012-11-27	Muqattash et al.	
294	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	295	8325638		2012-12-04	Jin, Haipeng et al.	
	296	8325906	B2	2012-12-04	Fullarton et al.	
	297	8326319	B2	2012-12-04	Davis, Richard W.	
	298	8326828	B2	2012-12-04	Zhou et al.	
	299	8331223	B2	2012-12-11	Hill et al.	
	300	8331293		2012-12-11	Sood, Kapil	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2414	
	Examiner Name	NOT YET ASSIGNED	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	1							☐
--	---	--	--	--	--	--	--	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	03/20/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

PTO/SB/08a (01-22)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	8332375		2012-12-11	Chatley, Scott P. et al.	
	2	8339991	B2	2012-12-25	Biswas et al.	
	3	8340625	B1	2012-12-25	Johnson et al.	
	4	8340678	B1	2012-12-25	Pandey, Vinod	
	5	8340718		2012-12-25	Colonna, Massimo et al.	
	6	8346210	B2	2013-01-01	Balsan et al.	
	7	8346923	B2	2013-01-01	Rowles et al.	
	8	8347104	B2	2013-01-01	Pathiyai, Krishna K.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

9	8347378	B2	2013-01-01	Merkin et al.	
10	8350700		2013-01-08	Fast, Raymond D. et al.	
11	8351592	B2	2013-01-08	Freeny Jr et al.	
12	8351898	B2	2013-01-08	Raleigh	
13	8352360	B2	2013-01-08	De Judicibus et al.	
14	8352980		2013-01-08	Howcroft, Jerald Robert	
15	8355696	B1	2013-01-15	Olding et al.	
16	8356336	B2	2013-01-15	Johnston, Keith et al.	
17	8358638	B2	2013-01-22	Scherzer, Tamir et al.	
18	8358975	B2	2013-01-22	Bahl et al.	
19	8363658		2013-01-29	Delker, Jason R. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

20	8363799	B2	2013-01-29	Gruchala et al.	
21	8364806		2013-01-29	Short, Joel E. et al.	
22	8370477		2013-02-05	Short, Joel E. et al.	
23	8370483	B	2013-02-05	Choong Jason et al.	
24	8374090		2013-02-12	Morrill, Robert J. et al.	
25	8374592		2013-02-12	Proctor, Jr. James A. et al.	
26	8375128	B2	2013-02-12	Tofighbakhsh et al.	
27	8375136	B2	2013-02-12	Roman et al.	
28	8380247	B2	2013-02-19	Engstrom	
29	8385199	B1	2013-02-26	Coward et al.	
30	8385896		2013-02-26	Proctor Jr., James A. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

31	8385964	B2	2013-02-26	Haney, Richard D.	
32	8386386		2013-02-26	Zhu, Kevin	
33	8392982	B2	2013-03-05	Harris et al.	
34	8396929		2013-03-12	Helfman, Nadav et al.	
35	8401906	B2	2013-03-19	Ruckart	
36	8401968	B1	2013-03-19	Schattauer et al.	
37	8402165	B2	2013-03-19	Deu-Ngoc et al.	
38	8402540		2013-03-19	Kapoor, Harsh et al.	
39	8406736	B2	2013-03-26	Das et al.	
40	8407763	B2	2013-03-26	Weller et al.	
41	8411587		2013-04-02	Curtis, William et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	8411691	B2	2013-04-02	Aggarwal	
43	8413245	B2	2013-04-02	Kraemer et al.	
44	8418168	B2	2013-04-09	Tyhurst et al.	
45	8423016		2013-04-16	BUCKLEY, Adrian et al.	
46	8429403		2013-04-23	Moret, Eric et al.	
47	8437734		2013-05-07	Ray, Amar N. et al.	
48	8442015	B2	2013-05-14	Behzad et al.	
49	8446831	B2	2013-05-21	Kwan et al.	
50	8447607	B2	2013-05-21	Weider, Chris et al.	
51	8447980		2013-05-21	Godfrey, James A. et al.	
52	8448015	B2	2013-05-21	Gerhart, David	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	8461958	B2	2013-06-11	Saenz et al.	
54	8463194	B2	2013-06-11	Erlenback et al.	
55	8463232	B2	2013-06-11	Tuli et al.	
56	8468337	B2	2013-06-18	Gaur, Santosh P. et al.	
57	8472371		2013-06-25	Bari, Farooq et al.	
58	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
59	8483135		2013-07-09	Cai, Yigang et al.	
60	8483694	B2	2013-07-09	Lewis et al.	
61	8484327	B2	2013-07-09	Werner et al.	
62	8488597	B2	2013-07-16	Nie et al.	
63	8489110	B2	2013-07-16	Frank et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	64	8489720	B1	2013-07-16	Morford, Michael et al.	
	65	8494559	B1	2013-07-23	Malmi	
	66	8495181	B2	2013-07-23	Venkatraman et al.	
	67	8495227		2013-07-23	Kaminsky, David L. et al.	
	68	8495360		2013-07-23	Falk, Rainer et al.	
	69	8495700	B2	2013-07-23	Shahbazi	
	70	8495743	B2	2013-07-23	Kraemer et al.	
	71	8500533	B2	2013-08-06	Lutnick et al.	
	72	8503358	B2	2013-08-06	Hanson et al.	
	73	8503455	B2	2013-08-06	Heikens, Heico	
	74	8504032	B2	2013-08-06	Lott et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

75	8504574	B2	2013-08-06	Dvorak et al.	
76	8504687	B2	2013-08-06	Maffione et al.	
77	8504729		2013-08-06	Pezzutti, David A.	
78	8505073	B2	2013-08-06	Taglienti et al.	
79	8509082	B2	2013-08-13	Heinz, John M. et al.	
80	8514927	B2	2013-08-20	Sundararajan et al.	
81	8520589		2013-08-27	Bhatt, Yogesh et al.	
82	8521110		2013-08-27	Rofougaran, Ahmadreza	
83	8521775	B1	2013-08-27	Poh et al.	
84	8522039	B2	2013-08-27	Hyndman et al.	
85	8522249	B2	2013-08-27	Beaule, Stephane	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2414	
	Examiner Name	NOT YET ASSIGNED	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	86	8522337	B2	2013-08-27	Adusumilli et al.	
	87	8523547	B2	2013-09-03	Pekrul, Merton W.	
	88	8526329	B2	2013-09-03	Mahany, Ronald L. et al.	
	89	8526350	B2	2013-09-03	Xue, Qi et al.	
	90	8527410	B2	2013-09-03	Markki et al.	
	91	8527662	B2	2013-09-03	Biswas et al.	
	92	8528068	B1	2013-09-03	Weglein et al.	
	93	8531954	B2	2013-09-10	McNaughton et al.	
	94	8531995	B2	2013-09-10	Khan et al.	
	95	8532610	B2	2013-09-10	Manning Cassett et al.	
	96	8533775	B2	2013-09-10	Alcorn et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

97	8535160	B2	2013-09-17	Lutnick et al.	
98	8538394	B2	2013-09-17	Zimmerman et al.	
99	8538421	B2	2013-09-17	Brisebois et al.	
100	8538458	B2	2013-09-17	Haney, Richard D.	
101	8539544	B2	2013-09-17	Garimella et al.	
102	8543265	B2	2013-09-24	Ekhuagere et al.	
103	8543814	B2	2013-09-24	Laitinen et al.	
104	8544105	B2	2013-09-24	McLean et al.	
105	8548427	B2	2013-10-01	Chow et al.	
106	8554876	B2	2013-10-08	Winsor, Gerald W.	
107	8559369	B2	2013-10-15	Barkan	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

108	8561138	B2	2013-10-15	Rothman, Michael M. et al.	
109	8565746	B2	2013-10-22	Hoffman, George E.	
110	8566236	B2	2013-10-22	Busch, James David	
111	8571474	B2	2013-10-29	Chavez et al.	
112	8571501	B2	2013-10-29	Miller et al.	
113	8571598	B2	2013-10-29	Vaiavi, John J.	
114	8571993	B2	2013-10-29	Kocher et al.	
115	8572117	B2	2013-10-29	Rappaport, Theodore S.	
116	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
117	8583499		2013-11-12	De Judicibus, Dario et al.	
118	8588240	B2	2013-11-19	Ramankutty et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

119	8589955	B2	2013-11-19	Roundtree et al.	
120	8594665	B2	2013-11-26	Anschutz, Thomas	
121	8595186	B1	2013-11-26	Mandyam et al.	
122	8600895	B2	2013-12-03	Felsher, David Paul	
123	8601125	B2	2013-12-03	Huang et al.	
124	8605691	B2	2013-12-10	Soomro et al.	
125	8611919	B2	2013-12-17	Barnes Jr.	
126	8615507	B2	2013-12-24	VARADARAJULU et al.	
127	8620257	B2	2013-12-31	Qiu et al.	
128	8634425	B2	2014-01-21	Gorti et al.	
129	8635164	B2	2014-01-21	Rosenhaft et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

130	8639215	B2	2014-01-28	McGregor et al.	
131	8644702	B1	2014-02-04	Kalajan, Kevin E.	
132	8644813	B1	2014-02-04	Gailloux et al.	
133	8645518	B	2014-02-04	David, Scott L.	
134	8655357	B1	2014-02-18	Gazzard et al.	
135	8656472	B2	2014-02-18	McMurtry et al.	
136	8660853	B2	2014-02-25	Robb et al.	
137	8666395	B2	2014-03-04	Silver, Andrew	
138	8667542	B1	2014-03-04	Bertz et al.	
139	8670334	B	2014-03-11	Keohane et al.	
140	8675852	B2	2014-03-18	Maes, Stephane H.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

141	8676682	B2	2014-03-18	Kalliola, Janne	
142	8676925	B	2014-03-18	Liu et al.	
143	8693323		2014-04-08	McDysan, David E.	
144	8694772	B2	2014-04-08	Kao et al.	
145	8700729	B2	2014-04-15	Dua, Robin	
146	8701015	B2	2014-04-15	Bonnat, Pierre	
147	8706863		2014-04-22	Fadell, Anthony	
148	8713535	B2	2014-04-29	Malhotra et al.	
149	8713641	B1	2014-04-29	Pagan et al.	
150	8719397	B2	2014-05-06	Levi et al.	
151	8719423	B2	2014-05-06	Wyld	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

152	8725899	B	2014-05-13	Short et al.	
153	8730842	B2	2014-05-20	Collins et al.	
154	8731519	B2	2014-05-20	Flynn et al.	
155	8732808	B2	2014-05-20	Sewall et al.	
156	8739035	B2	2014-05-27	Trethewey, Jim	
157	8744339	B2	2014-06-03	Halfmann et al.	
158	8761711	B2	2014-06-24	Grignani et al.	
159	8761809	B2	2014-06-24	Faith et al.	
160	8780857	B2	2014-07-15	Balasubramanian et al.	
161	8787249	B2	2014-07-22	Giaretta et al.	
162	8793304	B2	2014-07-29	Lu et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

163	8798610	B2	2014-08-05	Prakash et al.	
164	8804695	B2	2014-08-12	Branam	
165	8811338	B2	2014-08-19	Jin et al.	
166	8811991	B2	2014-08-19	Jain et al.	
167	8818394	B2	2014-08-26	Bienas et al.	
168	8819253	B2	2014-08-26	Simeloff et al.	
169	8825109	B2	2014-09-02	Montemurro et al.	
170	8826411	B2	2014-09-02	Moen et al.	
171	8831561	B2	2014-09-09	Sutaria et al.	
172	8838752	B2	2014-09-16	Lor et al.	
173	8845415	B2	2014-09-30	Lutnick et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

174	8849297	B2	2014-09-30	Balasubramanian	
175	8855620	B2	2014-10-07	Sievers et al.	
176	8862751	B2	2014-10-14	Faccin et al.	
177	8875042	B2	2014-10-28	LeJeune et al.	
178	8880047	B2	2014-11-04	Konicek et al.	
179	8908516	B2	2014-12-09	Tzamaloukas et al.	
180	8929374	B2	2015-01-06	Tönsing et al.	
181	8930238	B2	2015-01-06	Coffman et al.	
182	8943551	B2	2015-01-27	Ganapathy et al.	
183	8948726	B2	2015-02-03	Smith et al.	
184	8949382	B2	2015-02-03	Cornett et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

185	8955038	B2	2015-02-10	Nicodemus et al.	
186	8966018	B2	2015-02-24	Bugwadia et al.	
187	8971912	B2	2015-03-03	Chou et al.	
188	8977284	B2	2015-03-10	Reed, Mark J.	
189	8995952	B1	2015-03-31	Baker et al.	
190	9002342	B2	2015-04-07	Tenhunen et al.	
191	9014973	B2	2015-04-21	Ruckart, John	
192	9015331	B2	2015-04-21	Lai et al.	
193	9030934	B2	2015-05-12	Shah et al.	
194	9049010		2015-06-02	Jueneman et al.	
195	9064275	B1	2015-06-23	Lu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	196	9105031	B2	2015-08-11	Shen et al.	
	197	9111088	B2	2015-08-18	Ghai et al.	
	198	9137286	B1	2015-09-15	Yuan	
	199	9172553	B2	2015-10-27	Dawes et al.	
	200	9262370	B2	2016-02-16	Hofstaedter et al.	
	201	9286469	B2	2016-03-15	Kraemer et al.	
	202	9286604	B2	2016-03-15	Aabye et al.	
	203	9313708	B2	2016-04-12	Nam et al.	
	204	9325737	B2	2016-04-26	Gulowski et al.	
	205	9326173	B2	2016-04-26	Luft, Achim	
	206	9344557	B2	2016-05-17	Gruchala et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

207	9363285	B2	2016-06-07	Kitamura	
208	9367680	B2	2016-06-14	Mahaffey et al.	
209	9413546	B2	2016-08-09	Meier et al.	
210	9418381	B2	2016-08-16	Ahuja et al.	
211	9501803	B2	2016-11-22	Bilac et al.	
212	9516456	B2	2016-12-06	Stephens et al.	
213	9589117	B2	2017-03-07	Ali et al.	
214	9615192	B2	2017-04-04	Raleigh	
215	RE44412		2013-08-06	Naqvi et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
-------------------	---------	--------------------	------------------------	------------------	---	--

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

1						
---	--	--	--	--	--	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	03/20/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Receipt date: 06/11/2024

17/577,237 - GAU: 2633

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C	

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add
NON-PATENT LITERATURE DOCUMENTS								Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C

/F.M./	1	IPR2024-00342 PATENT OWNER'S PRELIMINARY RESPONSE, dated April 30, 2024	☐
/F.M./	2	IPR2024-00010 Decision Granting Institution of Inter Partes Review, dated May 23, 2024	☐
/F.M./	3	IPR2024-00003 PATENT OWNER'S PRELIMINARY RESPONSE, dated February 28, 2024,	☐
/F.M./	4	IPR2024-00003 Decision Denying Institution of Inter Partes Review, dated May 22, 2024	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	06/25/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-06-11
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/C6a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2633
	Examiner Name	Murillo Garcia, Fabricio R.
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code:	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/F.M./	1	8285850		2012-10-09	Jones, Nathan et al.	
/F.M./	2	8400491		2013-03-19	Panpaliya; Monika et al.	
/F.M./	3	5987611		1999-11-16	Freund; Gregor	
/F.M./	4	8019868		2011-09-13	Rao; Goutham et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code:	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/F.M./	1	20060039354		2006-02-23	Rao; Goutham P. et al.	
/F.M./	2	20090207817		2009-08-20	Montemurro; Michael et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	3	20090185527		2009-07-23	Akhtar; Haseeb et al.	
	4	20080162981		2008-07-03	Jajoo; Sandesh R. et al.	
	5	20090228951		2009-09-10	Ramesh; Tirumale K. et al.	
	6	20070032230		2007-02-08	Pregont; Gary J.	
	7	20060282566		2006-12-14	Virdi; Gurpratap et al.	
	8	20050080904		2005-04-14	Green, Dustin L.	
	9	20070121615		2007-05-31	Weill; Ofer et al.	
	10	20080080458		2008-04-03	COLE; TERRY L.	
	11	20100281154		2010-11-04	Bedi; Bharat Veer et al.	
	12	20070258459		2007-11-08	Smith; Donald L. et al.	
	13	20080122796		2008-05-29	Jobs; Steven P. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

/F.M./	14	20080002652		2008-01-03	Gupta; Dev V. et al.	
--------	----	-------------	--	------------	----------------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/F.M./	1	Complaint for Patent Infringement in Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2-23-cv-00641 (EDTX), Dec. 29, 2023)	☐
/F.M./	2	File History of IPR2024-01051, filed June 18, 2024	☐
/F.M./	3	IPR2024-01051 Inter Parties Review Petition, filed June 18, 2024	☐
/F.M./	4	van Beek, et. al., 2004, January. Adaptive streaming of high quality video over wireless LANs. In Visual Communications and Image Processing 2004 (Vol. 5308, pp. 647-660). SPIE.	☐
/F.M./	5	IETF RFC 791, Internet Protocol, September 1981, downloaded from the internet at https://www.ietf.org/rfc/rfc791.txt on July 28, 2023	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2633
Examiner Name	Murillo Garcia, Fabricio R.
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

6	IETF RFC 5246, The Transport Layer Security (TLS) Protocol, version 1.2, August 2008, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc5246 on May 9, 2024	☐
7	Internet connection speed recommendations, downloaded from the Internet at https://help.netflix.com/en/node/306 on April 29, 2024.	☐
8	Apostolopoulos, et al., 2002. Video streaming: Concepts, algorithms, and systems. HP Laboratories, report HPL-2002-260, pp.2641-8770.	☐
9	IETF RFC 793, TRANSMISSION CONTROL PROTOCOL, September 1981, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc793 on April 24, 2024.	☐
10	Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298.	☐
11	Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39.	☐
12	Banchs, et. al., Distributed weighted fair queuing in 802.11 wireless LAN, 2002 IEEE International Conference on Communications, Conference Proceedings. ICC 2002 pp. 3121-3127), 2002	☐
13	Wu, et. al., 2001. Scalable video coding and transport over broadband wireless networks. Proceedings of the IEEE, 89 (1), pp.6-20.	☐
14	IETF RFC 2205, Resource ReSerVation Protocol (RSVP), version 1 Functional Specification, September 1997, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2205 on May 16, 2024	☐
15	Excerpts, Computer Networks, Fourth Edition, by Andrew Tanenbaum, Prentice Hall, 2003	☐
16	Agrawal, et. al., 2005. Policy-based management of networked computing systems. IEEE Communications Magazine, 43(10), pp.69-75	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2633
Examiner Name	Murillo Garcia, Fabricio R.
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

17	Blake, et al., IETF RFC 2475, "An Architecture for Differentiated Services," December 1998, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2475 on July 29, 2023	☐
18	Reeder, et. al., 2007. Usability challenges in security and privacy policy-authoring interfaces. In Human-Computer Interaction-INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II 11 (pp. 141-155). Springer Berlin Heidelberg.	☐
19	Mansour, et al., 2001. Jitter control in QoS networks. IEEE/ACM Transactions On Networking, 9(4), pp.492-502.	☐
20	Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024.	☐
21	Damianou, et al., 2001. The ponder policy specification language. In Policies for Distributed Systems and Networks: International Workshop, POLICY 2001 Bristol, UK, January 29-31, 2001 Proceedings (pp. 18-38). Springer Berlin Heidelberg.	☐
22	Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach. IEEE network, 15(1), pp.10-21.	☐
23	Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39). IEEE.	☐
24	Simplified Policy Language (CIM-SPL). Document Number DSP0231, version, 1.	☐
25	Ponnappan, et al., 2002, June. A policy based QoS management system for the IntServ/DiffServ based Internet. In Proceedings Third International Workshop on Policies for Distributed Systems and Networks (pp. 159-168). IEEE.	☐
26	Gonçalves, et al., 2009, October. A graphical user interface for policy composition in CIM-SPL. In 2009 International Conference on Ultra Modern Telecommunications & Workshops (pp. 1-7). IEEE.	☐
27	Grossman, Invention of the year: The iPhone. Time Magazine Online, 1. downloaded from the internet at https://content.time.com/time/specials/2007/article/0,28804,1677329_1678542_1677891,00.html on May 28, 2024.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

/F.M./28	Excerpts, Telcom Dictionary, Aithos Publishing, 2007.	☐
----------	---	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	06/25/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2633
	Examiner Name	Murillo Garcia, Fabricio R.
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-06-19
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 17/577,237		Filing Date 01/17/2022		☐ To be Mailed	
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO									
APPLICATION AS FILED - PART I									
	(Column 1)	(Column 2)							
FOR	NUMBER FILED	NUMBER EXTRA			RATE (\$)			FEE (\$)	
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A			N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A				
TOTAL CLAIMS (37 CFR 1.16(j))	minus 20 =	*			x \$50 =				
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*			x \$240 =				
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))									
* If the difference in column 1 is less than zero, enter "0" in column 2.							TOTAL		
APPLICATION AS AMENDED - PART II									
	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	07/18/2024	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(j))	* 15	Minus	** 20	= 0		x \$40 =	0	
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x \$192 =	0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE	0		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(j))	*	Minus	**	=		x \$0 =		
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x \$0 =		
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LIE			
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/ALLYSON PURNELL/			
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".									
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.									

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh, Gregory G. Application Serial No.: 17/577,237 Filed: 1/17/2022 Title: Automated Device Provisioning and Activation	Group Art Unit: 2633 Examiner: Murillo Garcia, Fabricio R.
--	---

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This is in response to the *Final* Office Action, dated July 18, 2024, in the above-referenced patent application. Please enter and consider the following amendments and remarks.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 06/19/2024 06:47:44 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	66034578	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1 C1C1_IDS_June_19_24.pdf	878	-	12794 KB
RALEP007C11C3C2C3C2C 1C1C1_IDS_June_19_24- IDS.pdf	(1-7) 7	Information Disclosure Statement (IDS) Form (SB08)	11945 KB
RALEP007C11C3C2C3C2C 1C1C1_IDS_June_19_24- NPL.pdf	(8-878) 871	Non Patent Literature	12555 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C 1C1_IDS_June_19_24.pdf	B017D6833EFC7CE50F705D98D00E9108902FE770A54AD7FF2 893964088C8363983BC41F87962C20CE8CFE407B08BB09A1A9 6A673BE2BC916DF9C4F7F28FCF498
RALEP007C11C3C2C3C2C1C 1C1_IDS_June_19_24-IDS.pdf	9C2B55703F450F39E6A28EF6B44CDB091F735AB99A6CD5141 40C1CA91CED7DDAF5E7154320DCDCA7387CDD1F7D3D0F58 CD22C7347E97216DD88232379FF36691
RALEP007C11C3C2C3C2C1C 1C1_IDS_June_19_24-NPL.pdf	BCFD6BD2C695780A46A49A06C665875BFBB297EF6332B306F A80DC789D71976E2AD2B52909F14BF0A1A1C64DA8BA647397 A3406F23063251D3F8B344A10252BB

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/C6a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2633	
	Examiner Name		Murillo Garcia, Fabricio R.	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code*	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	8285850		2012-10-09	Jones, Nathan et al.	
	2	8400491		2013-03-19	Panpaliya; Monika et al.	
	3	5987611		1999-11-16	Freund; Gregor	
	4	8019868		2011-09-13	Rao; Goutham et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code*	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20060039354		2006-02-23	Rao; Goutham P. et al.	
	2	20090207817		2009-08-20	Montemurro; Michael et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	3	20090185527		2009-07-23	Akhtar; Haseeb et al.	
	4	20080162981		2008-07-03	Jajoo; Sandesh R. et al.	
	5	20090228951		2009-09-10	Ramesh; Tirumale K. et al.	
	6	20070032230		2007-02-08	Pregont; Gary J.	
	7	20060282566		2006-12-14	Virdi; Gurpratap et al.	
	8	20050080904		2005-04-14	Green, Dustin L.	
	9	20070121615		2007-05-31	Weill; Ofer et al.	
	10	20080080458		2008-04-03	COLE; TERRY L.	
	11	20100281154		2010-11-04	Bedi; Bharat Veer et al.	
	12	20070258459		2007-11-08	Smith; Donald L. et al.	
	13	20080122796		2008-05-29	Jobs; Steven P. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2633	
	Examiner Name		Murillo Garcia, Fabricio R.	
Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1		

	14	20080002652		2008-01-03	Gupta; Dev V. et al.	
--	----	-------------	--	------------	----------------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Complaint for Patent Infringement in Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2-23-cv-00641 (EDTX), Dec. 29, 2023)	☐
	2	File History of IPR2024-01051, filed June 18, 2024	☐
	3	IPR2024-01051 Inter Parties Review Petition, filed June 18, 2024	☐
	4	van Beek, et. al., 2004, January. Adaptive streaming of high quality video over wireless LANs. In Visual Communications and Image Processing 2004 (Vol. 5308, pp. 647-660). SPIE.	☐
	5	IETF RFC 791, Internet Protocol, September 1981, downloaded from the internet at https://www.ietf.org/rfc/rfc791.txt on July 28, 2023	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

6	IETF RFC 5246, The Transport Layer Security (TLS) Protocol, version 1.2, August 2008, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc5246 on May 9, 2024	☐
7	Internet connection speed recommendations, downloaded from the Internet at https://help.netflix.com/en/node/306 on April 29, 2024.	☐
8	Apostolopoulos, et al., 2002. Video streaming: Concepts, algorithms, and systems. HP Laboratories, report HPL-2002-260, pp.2641-8770.	☐
9	IETF RFC 793, TRANSMISSION CONTROL PROTOCOL, September 1981, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc793 on April 24, 2024.	☐
10	Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298.	☐
11	Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39.	☐
12	Banchs, et. al., Distributed weighted fair queuing in 802.11 wireless LAN, 2002 IEEE International Conference on Communications, Conference Proceedings. ICC 2002 pp. 3121-3127), 2002	☐
13	Wu, et. al., 2001. Scalable video coding and transport over broadband wireless networks. Proceedings of the IEEE, 89 (1), pp.6-20.	☐
14	IETF RFC 2205, Resource ReSerVation Protocol (RSVP), version 1 Functional Specification, September 1997, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2205 on May 16, 2024	☐
15	Excerpts, Computer Networks, Fourth Edition, by Andrew Tanenbaum, Prentice Hall, 2003	☐
16	Agrawal, et. al., 2005. Policy-based management of networked computing systems. IEEE Communications Magazine, 43(10), pp.69-75	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2633
	Examiner Name	Murillo Garcia, Fabricio R.
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

17	Blake, et al., IETF RFC 2475, "An Architecture for Differentiated Services," December 1998, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2475 on July 29, 2023	☐
18	Reeder, et. al., 2007. Usability challenges in security and privacy policy-authoring interfaces. In Human-Computer Interaction-INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II 11 (pp. 141-155). Springer Berlin Heidelberg.	☐
19	Mansour, et al., 2001. Jitter control in QoS networks. IEEE/ACM Transactions On Networking, 9(4), pp.492-502.	☐
20	Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024.	☐
21	Damianou, et al., 2001. The ponder policy specification language. In Policies for Distributed Systems and Networks: International Workshop, POLICY 2001 Bristol, UK, January 29-31, 2001 Proceedings (pp. 18-38). Springer Berlin Heidelberg.	☐
22	Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach. IEEE network, 15(1), pp.10-21.	☐
23	Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39). IEEE.	☐
24	Simplified Policy Language (CIM-SPL). Document Number DSP0231, version, 1.	☐
25	Ponnappan, et al., 2002, June. A policy based QoS management system for the IntServ/DiffServ based Internet. In Proceedings Third International Workshop on Policies for Distributed Systems and Networks (pp. 159-168). IEEE.	☐
26	Gonçalves, et al., 2009, October. A graphical user interface for policy composition in CIM-SPL. In 2009 International Conference on Ultra Modern Telecommunications & Workshops (pp. 1-7). IEEE.	☐
27	Grossman, Invention of the year: The iPhone. Time Magazine Online, 1. downloaded from the internet at https://content.time.com/time/specials/2007/article/0,28804,1677329_1678542_1677891,00.html on May 28, 2024.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2633	
	Examiner Name	Murillo Garcia, Fabricio R.	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	28	Excerpts, Telcom Dictionary, Aithos Publishing, 2007.	☐
--	----	---	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2633
Examiner Name	Murillo Garcia, Fabricio R.
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-06-19
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 06/11/2024 06:15:52 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	65925111	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 5

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1 C1C1 IDS.pdf	4	Information Disclosure Statement (IDS) Form (SB08)	1252 KB
IPR2024-00342 PATENT OWNER PRELIMINARY RESPONSE.pdf	16	Non Patent Literature	188 KB
IPR2024-00010 Decision Granting Institution of Inter Partes Review.pdf	30	Non Patent Literature	754 KB
IPR2024-00003 PATENT OWNERS PRELIMINARY RESPONSE.pdf	52	Non Patent Literature	1158 KB

IPR2024-00003 Decision Denying Institution of Inter PartesReview.pdf	42	Non Patent Literature	647 KB
--	----	-----------------------	--------

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C 1C1 IDS.pdf	09CF772DA58FBE9033EC978F16D5EAE4ED9D81841E94642C4 2B6CCC34B9ED1607613CF728CCE07EF003C5969D190C3A764 3BD8A20C6E4658722BE60240C19B10
IPR2024-00342 PATENT OWNER PRELIMINARY RESPONSE.pdf	DA99CB1B5EC66E693E130C845910F005346BA438DB1F957B5 1CF803E310D3A445AA34F99781966FF93B5DE7C91F579A1C66 F5E2217086174D988CB8F8593DB29
IPR2024-00010 Decision Granting Institution of Inter PartesReview.pdf	864C02F796BCE069BB013D08C3BF705F2C27CAF1A854F83B6 CC7FB3E6FB1D25130C7C6D11857CFD83E8924FA43F4F0EB9 A3DF5B3E9433C51A41558ABEAFD8C5C
IPR2024-00003 PATENT OWNERS PRELIMINARY RESPONSE.pdf	5C9DB08A0E349316664D97CC004480804C189E8296336DC301 43F7EFCF1C753385F64BE7C95BE043C54B4CE3C27FC499950 031BBAE7870DB0844D528006E1F6F
IPR2024-00003 Decision Denying Institution of Inter PartesReview.pdf	4057DFA536B45D58B5DFE2E3536156CC1655F9282983938E1E E7E7C9C0077F8CED1025F62A70A7123AB012B4F29ECAD9BE B691452E0C5FC49AE2CF8D1AAC20BA

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add
NON-PATENT LITERATURE DOCUMENTS								Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C	

	1	IPR2024-00342 PATENT OWNER'S PRELIMINARY RESPONSE, dated April 30, 2024	☐
	2	IPR2024-00010 Decision Granting Institution of Inter Partes Review, dated May 23, 2024	☐
	3	IPR2024-00003 PATENT OWNER'S PRELIMINARY RESPONSE, dated February 28, 2024,	☐
	4	IPR2024-00003 Decision Denying Institution of Inter Partes Review, dated May 22, 2024	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

***EXAMINER:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C

CERTIFICATION STATEMENT			
Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):			
☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).			
OR			
☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).			
☐ See attached certification statement.			
☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.			
☒ A certification statement is not submitted herewith.			
SIGNATURE			
A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.			
Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-06-11
Name/Print	Farshad Farjami	Registration Number	41014
<p>This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.</p>			

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 06/04/2024 08:46:59 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	65828443	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1 C1C1_Resp_to_Non_Final_O A_June_4_24.pdf	9	-	69 KB
RALEP007C11C3C2C3C2C 1C1C1_Resp_to_Non_Final _OA_June_4_24- TRAN.LET.pdf	(1-1) 1	Transmittal Letter	30 KB
RALEP007C11C3C2C3C2C 1C1C1_Resp_to_Non_Final _OA_June_4_24-A....pdf	(2-9) 8	Amendment/Request for Reconsideration-After Non- Final Rejection	51 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
RALEP007C11C3C2C3C2C1C 1C1_Resp_to_Non_Final_OA_J une_4_24.pdf	38BF29BCC6F2202B5F9DFC1495D5F57BD4839363B67C18EB7 2382DB61B4438913AAF71AAC81874D0FBB2ED53CF3D74E089 F6C4A65802CCA13B960515E705FA03
RALEP007C11C3C2C3C2C1C 1C1_Resp_to_Non_Final_OA_J une_4_24-TRAN.LET.pdf	8C864E22CAA7CF2EDAA21599A12996125908839A047B1396F5 722CB0DACCD83DD27280A80B415C3FE947A5FB8F173BF6E6 3DFB34CCB09F3A4A393C214C6703B1
RALEP007C11C3C2C3C2C1C 1C1_Resp_to_Non_Final_OA_J une_4_24-A....pdf	AB5C97EF3ECB5418F9C6B8345E0F312FA7AF2BABD326BBD1 F1D1F7522B83D891C9CFA0DF107EF9D4442443D0E4455F9DD 15A7063A1074A6E78E4CFFF50513DA2

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: June 4, 2024

To: United States Patent and Trademark Office
Examiner: Murillo Garcia, Fabricio R.; Art Unit: 2633

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 9

Message:

Enclosed, please find the Amendment and Response to Non-Final Office Action, dated March 18, 2024.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain PRIVILEGED AND CONFIDENTIAL information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh, Gregory G. Application Serial No.: 17/577,237 Filed: 1/17/2022 Title: Automated Device Provisioning and Activation	Group Art Unit: 2633 Examiner: Murillo Garcia, Fabricio R.
--	---

AMENDMENT AND RESPONSE TO *NON-FINAL* OFFICE ACTION

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This is in response to the *Non-Final* Office Action, dated March 18, 2024, in the above-referenced patent application. Please enter and consider the following amendments and remarks.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.

In the Claims:

Claim 1 (Cancelled)

Claim 2 (New): A network message server adapted to communicate with a mobile end-user device having a plurality of applications, the network message server comprising:

one or more processors configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the request corresponding to a first application of the plurality of application;

generate an Internet data message based on the request, the Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the Internet data message to the mobile end-user device for mapping the first application identifier included in the Internet data message to the first application corresponding to the first application identifier, and forwarding the application data in the Internet data message to the mapped application.

Claim 3 (New): The network message server of claim 2, wherein the one or more processors are further configured to:

encrypt the secure Internet data message to generate encrypted secure Internet data message.

Claim 4 (New): The network message server of claim 2, wherein the secure Internet data message is transmitted using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, or tunneling.

Claim 5 (New): The network message server of claim 2, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 6 (New): The network message server of claim 2, wherein the one or more processors are further configured to:

authenticate the first application prior to transmitting the Internet data message to the mobile end-user device.

Claim 7 (New): A method for use by a network message server adapted to communicate with a mobile end-user device having a plurality of applications, the method comprising:

providing a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receiving a request to transmit application data, the request corresponding to a first application of the plurality of application;

generating an Internet data message based on the request, the Internet data message including the application data and a first application identifier identifying the first application; and

transmitting, over the secure Internet data connection, the Internet data message to the mobile end-user device for mapping the first application identifier included in the Internet data message to the first application corresponding to the first application identifier, and forwarding the application data in the Internet data message to the mapped application.

Claim 8 (New): The method of claim 7, further comprising:
encrypting the secure Internet data message to generate encrypted secure Internet data message.

Claim 9 (New): The method of claim 7, wherein the secure Internet data message is transmitted using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, or tunneling.

Claim 10 (New): The method of claim 7, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 11 (New): The method of claim 7, further comprising:
authenticating the first application prior to transmitting the Internet data message to the mobile end-user device.

Claim 12 (New): A network system comprising:
a mobile end-user device having a plurality of applications;
a message server adapted to communicate with the mobile end-user device, the network message server configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the request corresponding to a first application of the plurality of application;

generate an Internet data message based on the request, the Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the Internet data message to the mobile end-user device;

the mobile end-user device configured to:

receive the Internet data message from the network message server;

map the first application identifier included in the Internet data message to the first application corresponding to the first application identifier; and

forwarding the application data in the Internet data message to the mapped application.

Claim 13 (New): The network system of claim 12, wherein the network message server is further configured to:

encrypt the secure Internet data message to generate encrypted secure Internet data message.

Claim 14 (New): The network system of claim 12, wherein the secure Internet data message is transmitted using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, or tunneling.

Claim 15 (New): The network system of claim 12, wherein the mobile end-user device initiates the secure Internet data connection to the network message server.

Claim 16 (New): The network system of claim 12, wherein the network message server is further configured to:

authenticate the first application prior to transmitting the Internet data message to the mobile end-user device.

REMARKS

The *Non-Final* Office Action, dated March 18, 2024 (“Office Action”), rejected claim 1. By the present response, Applicant cancels claim 1, and adds new claims 2-16. No new matter is added. Thus, after the present response, claims 2-16 remain pending in the present application. Applicant respectfully requests allowance of claims 2-16 in view of the following remarks.

A. Non-Statutory Obviousness-Type Double Patenting

The Office Action rejected claim 1 of the present application, under non-statutory obviousness-type double patenting. By the present amendment, Applicant has cancelled claim 1. Therefore, the rejection of claim 1 is rendered moot.

B. 35 U.S.C. § 102

The Office Action rejected claim 1 of the present application, under 35 U.S.C. § 102, as being anticipated by Gao et al. (U.S. Patent Publication No. 2009/0292815) (“Gao”). By the present amendment, Applicant has cancelled claim 1. Therefore, the rejection of claim 1 is rendered moot.

C. New Claims 2-16

By the present amendment, Applicant has added new independent claim 2, which recites “A network message server adapted to communicate with a mobile end-user device having a plurality of applications,” where the network message server comprises:

one or more processors configured to:

provide a secure Internet data connection with the mobile end-user device via a device data connection to a wireless network;

receive a request to transmit application data, the request corresponding to a first application of the plurality of application;

generate an Internet data message based on the request, the Internet data message including the application data and a first application identifier identifying the first application; and

transmit, over the secure Internet data connection, the Internet data message to the mobile end-user device for mapping the first application identifier included in the Internet data message to the first application corresponding to the first application identifier, and forwarding the application data in the Internet data message to the mapped application.

New independent claims 7 and 12 also recite similar limitations. Applicant respectfully submits that new independent claims 2, 7 and 12 are patentably distinguishable over Gao and other references of record for reciting the aforementioned limitations, and should be allowed. As such, claims 3-6, 8-11 and 13-16 depending from new independent claims 2, 7 and 12, respectively, should also be allowed.

D. Conclusion

Based on the foregoing reasons, Applicant respectfully requests allowance of claims 2-16 pending in the present application.

The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication, or credit any overpayment to Deposit Account No. 50-0731.

Respectfully Submitted,
FARJAMI & FARJAMI LLP

/Farshad Farjami/
Farshad Farjami
Reg. No. 41,014

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, California 92691
Telephone: (949) 282-1000
Facsimile: (949) 282-1002

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

June 4, 2024
Date

Evan C. Gunderman
Name

/evan c. gunderman/
Signature



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1	5850
106963	7590	03/18/2024		
Headwater Research LLC C/O Farjami & Farjami LLP 26522 La Alameda Ave., Suite 360 Mission Viejo, CA 92691			EXAMINER MURILLO GARCIA, FABRICIO R	
			ART UNIT 2633	PAPER NUMBER
			NOTIFICATION DATE 03/18/2024	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@farjami.com
ffarjami@farjami.com
patent@headwaterllc.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

The IDS submitted on **24 May 2024** is in compliance and has been considered. Examiner notes that, given the quantity and length of the references, only a cursory review has been performed until such time as Applicant provides a detailed explanation of relevance or specifically points out only those sections of relevance in the disclosure.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619

(CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit <http://www.uspto.gov/forms/>. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to <http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp>.

Claim 1 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 8,839,388.

Although the claims at issue are not identical, they are not patentably distinct from each other because claims of the instant application and/or claims of the issued patent merely broaden the scope of the claims of the issued patent and/or claims of the instant application. It has been held that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before (See MPEP §804.II.B.1 and §2144.04 IIA).

Claim 1 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 11,228,617.

Although the claims at issue are not identical, they are not patentably distinct from each other because claims of the instant application and/or claims of the issued patent merely broaden the scope of the claims of the issued patent and/or claims of the instant application. It has been held that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before (See MPEP §804.II.B.1 and §2144.04 IIA).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale or otherwise available to the public before the effective filing date of the claimed invention.

(a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

Claim 1 is rejected under 35 U.S.C. 102(a)(1)-(a)(2) as being anticipated by Gao et al. (US Patent Application Publication No. 2009/0292815).

Regarding claim 1, Gao teaches a system (Fig. 2), comprising:

a processor of a communications device (device processing apparatus

[Paragraphs 26, 48, 71]) **configured to:**

store a first set of device credentials for activating the communications device for a first service on a first network (device processing apparatus storing device credentials for access a network [Paragraph 71]); **and**

send an access request to the first network, the access request including the first set of device credentials (request is sent to the network including the access credentials [Paragraphs 19, 22]); **and**

a memory of the communications device coupled to the processor and configured to provide the processor with instructions (memory for providing instructions to processing device [Paragraphs 27-28, 65, 71]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FABRICIO R MURILLO GARCIA whose telephone number is (571)270-5708. The examiner can normally be reached 9-5pm.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sam K Ahn can be reached on 5712723044. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be

obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

March 9, 2024

/FABRICIO R MURILLO GARCIA/
Primary Examiner, Art Unit 2633

<i>Notice of References Cited</i>	Application/Control No. 17/577,237		Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.	
	Examiner FABRICIO R MURILLO GARCIA		Art Unit 2633	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Name	CPC Classification	US Classification
*	A	US-20090292815-A1	2009-11-26	Gao; Ji	G06Q30/06	709/227
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date YYYY-MM-DD	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in YYYY-MM-DD format are publication dates. Classifications may be US or foreign.

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

CPC - Searched*		
Symbol	Date	Examiner
G06F15/177	03/09/2024	FM
H04W28/0215	03/09/2024	FM

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
455/406		03/09/2024	FM

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
East (See Attachment)	03/09/2024	03/09/2024
Inventor Search (search for double patenting)	03/09/2024	03/09/2024
Non Patentable Literature	03/09/2024	03/09/2024
455/406 - See Attached East Search	03/09/2024	03/09/2024
G06F15/177 - See Attached East Search	03/09/2024	03/09/2024
H04W28/0215 - See Attached East Search	03/09/2024	03/09/2024

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

<i>Search Notes</i> 	Application/Control No. 17/577,237	Applicant(s)/Patent Under Reexamination Raleigh, Gregory G.
	Examiner FABRICIO R MURILLO GARCIA	Art Unit 2633

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/FABRICIO R MURILLO GARCIA/ Primary Examiner, Art Unit 2633	
--	--

Bibliographic Data

Application No: 17/577,237

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged:

/FABRICIO R MURILLO
GARCIA/

Examiner's Signature

Initials

Title:

Automated Device Provisioning and Activation

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
01/17/2022	455	2633	
RULE			

APPLICANTS

Headwater Research LLC, Tyler, TX,

INVENTORS

Gregory G. Raleigh, Incline Village, NV, UNITED STATES

CONTINUING DATA

This application is a CON of 16436628 06/10/2019 PAT 11228617

16436628 is a CON of 15582350 04/28/2017 PAT 10321320

15582350 is a CON of 15239398 08/17/2016 PAT 9641957

15239398 is a CON of 14979233 12/22/2015 PAT 9532161

14979233 is a CON of 14667353 03/24/2015 PAT 9232403

14667353 is a CON of 14263604 04/28/2014 PAT 9037127

14263604 is a CON of 12380780 03/02/2009 PAT 8839388

12380780 has PRO of 61207739 02/13/2009

12380780 has PRO of 61207393 02/10/2009

12380780 has PRO of 61206944 02/04/2009

12380780 has PRO of 61206354 01/28/2009

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

01/25/2022

** SMALL ENTITY **

STATE OR COUNTRY

UNITED STATES

ADDRESS

FILING FEE RECEIVED

\$2,070

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	3687		
	Examiner Name	Unknown		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/F.M./	1	7082615		2006-07-25	Ellison	
/F.M./	2	8041816		2011-10-18	Ozaki	
/F.M./	3	7925717		2011-04-12	Chou	
/F.M./	4	7509487		2009-03-24	Lu	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/F.M./	1	20070011736		2007-01-11	Kalibjian	
/F.M./	2	20090240807		2009-09-24	Munson	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		3687	
	Examiner Name		Unknown	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	3	20090282256		2009-11-12	Rakic	
	4	20040122907		2004-06-24	Chou	
	5	20040105431		2004-06-03	Monjas-Llorente	
	6	20070214245		2007-09-13	Hämäläinen	
	7	20050207379		2005-09-22	Shen	
	8	20060190720		2006-08-24	Ozaki	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2006077283	WO			Houghton		☐
	2	2008048075	WO			Lee		☐
	3	1853044	EP			Shenfield		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	3687
Examiner Name	Unknown
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Security Engineering "A Guide to Building Dependable Distributed Systems," second edition, 2005 by Ross J. Anderson	☐
	2	Internet Archive of CryptoGraf, accessed Sep. 20, 2023, available at https://web.archive.org/web/20070210050616/http://www.cryptograf.com/	☐
	3	National Institute of Standards and Technology (NIST) glossary of terms, accessed Sep. 20, 2023, available at https://csrc.nist.gov/glossary/term/aaa	☐
	4	Headwater Infringement Contentions for U.S. Patent No. 9,198,117 vis-a-vis Samsung's mobile electronic devices	☐
	5	Complaint, Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2:23-cv-00103, E.D. Tex., March 10, 2023	☐
	6	IPR2024-00003; Petition for Inter Partes Review of United States Patent No. 9,198,117, filed on November 17, 2023	☐
	7	IPR2024-00010; Petition for Inter Partes Review of United States Patent No. 9,615,192, filed on November 17, 2023	☐
	8	3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2 ("TS-23.140")	☐
	9	Open Mobile Alliance; Multimedia Messaging Service Architecture Overview (MMSARCH) specification, available at https://www.openmobilealliance.org/release/MMS/V1_1-20040715-A/OMA-WAP-MMS-ARCHV1_1-20040715-A.pdf	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	3687
Examiner Name	Unknown
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

10	Open Mobile Alliance; OMA-ERELD-MMS-v1_2-20030923-C, "Enabler Release Definition for MMS Version 1.2," available at https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMAERELD-MMS-V1_2-20030923-C.pdf	☐
11	Technical Specification Group Services and System Aspects Meeting #19, TSGS#19(03)0167, European Telecommunications Standards Institute February 2003 (available at https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_19/Docs/PDF/SP-030167.pdf)	☐
12	IETF RFC 793, Transmission Control Protocol (Sept. 1981) (available at https://www.ietf.org/rfc/rfc793.txt)	☐
13	The TLS Protocol Version v 1.0 (Jan. 1999) (available at https://datatracker.ietf.org/doc/html/rfc2246)	☐
14	Needham et al., "Using Encryption for Authentication in Large Networks of Computers" (ACM, Vol. 21, No. 12, Dec. 1978)	☐
15	Schroeder et al., "A Hardware Architecture for Implementing Protection Rings" (ACM, Vol. 15, No. 3, Mar. 1972)	☐
16	Saltzer et al., "The Protection of Information in Computer Systems" (IEEE Proceedings, Vol. 63, No. 9, Sept. 1975)	☐
17	Li et al., "Symbian OS platform security model," available at https://www.usenix.org/system/files/login/articles/73507-li.pdf (Login Magazine, Aug. 2010)	☐
18	Philip Zimmermann, "Pretty Good Privacy: RSA Public Key Cryptography for the Masses" PGP User's Guide. Version 1.0, June 1991), available at https://www.techinsider.org/free-software/research/acrobat/910605.pdf	☐
19	B. Ramsdell, S/MIME Version 3 Message Specification, IETF RFC 2633, June 1999, available at https://datatracker.ietf.org/doc/html/rfc2633	☐
20	Mostafa, "Transporting data between wireless applications using a messaging system—MMS" (Wireless Comms. and Mobile Computing, July 7, 2006)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	3687
	Examiner Name	Unknown
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

If you wish to add additional non-patent literature document citation information please click the Add button			
EXAMINER SIGNATURE			
Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	03/09/2024
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			
<small>¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.</small>			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	3687
	Examiner Name	Unknown
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2023-11-22
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Inventor Information

Inventor Name	Application Number #	Patent Number	PG Pub Number	Status	Title	Examiner Name	Date Filed
RALEIGH, GREGORY	09565688	6973154		150	OFDM INTERFERENCE CANCELLATION BASED ON TRAINING SYMBOL INTERFERENCE	FAICHEN	05/04/2000
RALEIGH, GREGORY	09749760	7988800		250	ADVANCE SIGNALING FOR MULTI STAGE TRANSCEIVERS	LEE,JOHN	12/21/2000
RALEIGH, GREGORY	11138581	7090791	20090271180	250	OFDM INTERFERENCE CANCELLATION BASED ON TRAINING SYMBOL INTERFERENCE	YIM,YEON	06/02/2001
RALEIGH, GREGORY	12459448	7787896		250	ADVANCED SIGNALING FOR MULTI STAGE TRANSCEIVERS	LEE,JOHN	06/01/2008
RALEIGH, GREGORY	13026801	8960113	20150420715	150	TRACKING OF TUMOR LOCATION FOR TARGETED RADIATION TREATMENT	LAMPH,JOSEPH DARYL	01/20/2012
RALEIGH, GREGORY	13089524	9293404	20120316428	150	IMAGING OBSERVATION TIMING FOR ASSISTING RADIATION TREATMENT	ROZANSKY,MICHAEL	07/18/2012
RALEIGH, GREGORY	13090052	Not Issued	20120312861	151	SETTING IMAGING PARAMETERS FOR IMAGE GUIDED RADIATION TREATMENT	CHAVEZ,RENEE	07/16/2012
RALEIGH, GREGORY	13090941	8848542	20150906050	150	RADIATION TREATMENT WITH MULTIPLE IMAGERS ELEMENTS	GATTUNGAL,SANJAY	07/16/2012
RALEIGH, GREGORY	13090544	Not Issued	20120316425	151	TIMING OF A PLURALITY OF IMAGING OBSERVATION ELEMENTS BASED ON A VOLUME OF INTEREST	WEATHERSV,ELLENWORTH	07/18/2012
RALEIGH, GREGORY	13090575	Not Issued	20120316379	151	IMAGERS OBSERVATION TIMING BASED ON RADIATION TREATMENT SYSTEM ELEMENT DELAY	COY,THADDEUS	07/16/2012
RALEIGH, GREGORY	13090980	9364587	20150906036	150	IMAGING OBSERVATION TIMING BASED ON RADIATION TREATMENT SYSTEM ELEMENT DELAY	COX,THADEUS	07/18/2012
RALEIGH, GREGORY	13093720	9824895	20120330823	150	DEVICE ASSISTED OUR CREATION AGGREGATION, MEDIATION AND BILLING	RODY,ANDREW	08/02/2012
RALEIGH, GREGORY	13094826	8930617	20150482501	150	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM	RILEY,ANDREW	10/19/2012
RALEIGH, GREGORY	13708320	9093510	20130238781	150	CONTENT DISTRIBUTION BASED ON A VALUE METRIC	WOOLCOCK,MADHU	03/07/2013
RALEIGH, GREGORY	13709308	9330225	20130238761	150	DISTRIBUTING CONTENT BY GENERATING AND PRELOADING QUEUES OF CONTENT	MUSANUR,RAD	03/07/2013
RALEIGH, GREGORY	13788402	9210217	20150298782	150	CONTENT BROKER THAT OFFERS PRELOADING OPPORTUNITIES	THREU,BENJAMIN	09/07/2013
RALEIGH, GREGORY	18093265	Not Issued	2020045127	151	Content Distribution Based on a Value Metric	WOOLCOCK,MADHU	07/11/2018
RALEIGH, GREGORY	61209844	Not Issued		159	Services policy communication system and method		02/04/2009
RALEIGH, GREGORY	61207393	Not Issued		158	Services policy communication system and method		02/10/2008
RALEIGH, GREGORY	61207738	Not Issued		159	Services policy communication system and method		02/19/2009

Doc code: IDS

PTO/SB/08a (01-22)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	3687
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S. PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20030229900	A1	2003-12-11	Reisman	
	2	20060135144	A1	2006-06-22	Jothipragasam	
	3	20080082643	A1	2008-04-03	Storrie et al.	
	4	20080124330	A1	2008-05-29	Nakano et al.	
	5	20080134330	A1	2008-06-05	Kapoor et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						
FOREIGN PATENT DOCUMENTS						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	3687	
	Examiner Name	NOT YET ASSIGNED	
Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1855817	CN	B	2012-07-04	Mcbride et al.		☐
	2	1247411	EP	A2	2002-10-09	Charas		☐
	3	1247411	EP	B1	2011-11-02	Charas		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	03/09/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	3687
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

- ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

- ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2023-02-10
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	1	"17577237"	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:06 AM
L2	633	((("RALEIGH") near3 ("Gregory"))).INV.	(US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT)	OR	ON	ON	2024/03/09 06:10 AM
L3	1	((US-20220279021-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:19 PM
L4	3098	(store) WITH ((device) near2 (credential))	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:36 PM
L5	2	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L6	0	(store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal) WITH (activate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:37 PM
L7	30	("6178511" "6243816" "7249182" "7296036" "7310515" "7346855" "7353462" "8472874" "8606854" "20040009750" "20040113807" "20050026594" "20050076124" "20050193093" "20050281237" "20060063548" "20060234631" "20070021111" "20070167136" "20070168425" "20070242814" "20070260751" "20080051033" "20080108308" "20090209202").pn. OR ("9357352").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:38 PM
L8	4	((US-11304026-B2 OR US-10963844-B2 OR US-10250549-B2 OR US-9609673-B2).did. AND USPT.dbnm.)	(USPAT)	OR	ON	ON	2024/03/09 06:38 PM
L9	4	((US-8606854-B2 OR US-8472874-B2).did.	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM

L10	4	AND USPT.dbnm.) OR ((US-20090209202-A1 OR US-20080108308- A1).did. AND PGPB.dbnm.) ((US-7353462-B2 OR US-7346855-B2 OR US-7296036-B2).did. AND USPT.dbnm.) OR ((US-20080051033- A1).did. AND PGPB.dbnm.)	(USPAT; US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L11	4	((US-20070260751-A1 OR US-20070242814- A1 OR US- 20070167136-A1 OR US-20070168425- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L12	4	((US-20070021111-A1 OR US-20060234631- A1 OR US- 20060063548-A1 OR US-20050281237- A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:38 PM
L13	41	("6867733" "7418268" "7686217" "7847684" "8010131" "8108414" "8655385" "8688143" "8892130" "9173245" "9203857" "9226105" "9268920" "9357352" "9485211" "9830562" "9940402" "10013489" "10049400" "10075822" "10078696" "10264609" "10575138" "10599390" "20040116106" "20100313142" "20130316735" "20130331087" "20140162698" "20150058427" "20150080027" "20150088672" "20150365787" "20150378587" "20160261985" "20160334545" "20160364811" "20180176166"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:39 PM

		"20190014220" "20190215660" "20210173880").pn. OR ("11304026").urpn. AND (PGPB USPT USOC).dbnm.					
L14	2	(storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L15	5	(stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L16	5	(save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:39 PM
L17	5	(saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L18	5	(saved saving save stored storing store) WITH ((device) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L19	6	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (mobile ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L20	30	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L21	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM
L22	66	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:40 PM

L23	72	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L24	75	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:41 PM
L25	759	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH ((mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L26	762	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L27	128	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:42 PM
L28	88	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L29	78	(user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L30	66	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L31	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L32	0	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activae)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L33	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM

L34	1	(user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L35	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:43 PM
L36	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (activate initiate start begin)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:44 PM
L37	1	("2022/0124167").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:45 PM
L38	2	((US-20220279021-A1 OR US-20160135014- A1).did. AND PGPB.dbnm.)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2024/03/09 06:45 PM
L39	1	(saved saving save stored storing store) near10 ((device sensor)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L40	1	near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start begin beginning) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L41	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L42	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start began began begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L43	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L44	1	near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L45	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM
L46	1	(saved saving save stored storing store) near10 ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:55 PM

L47	4	starting run activate initiate start started began begun begin beginning) (saved saving save stored storing store) WITH ((device sensor) near2 (credential)) near10 (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L48	3	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) near10 (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L49	4	(saved saving save stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) near10 (initiated initiating running starting run activate initiate start started began begun begin beginning)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:56 PM
L50	15	(saved saving save	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09

		stored storing store) WITH ((device sensor) near2 (credential)) WITH (handheld (mobile ADJ device) (user ADJ terminal) (user ADJ equipment) cellphone smartphone (mobile ADJ terminal) ue) WITH (network) WITH (initiated initiating running starting run activate initiate start started began begun begin beginning)					06:56 PM
L51	4	((US-20220124167-A1 OR US-20200275225- A1 OR US- 20170006034-A1).did. AND PGPB.dbnm.) OR ((US-9554061-B1).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 06:59 PM
L52	3	((US-20140373012-A1 OR US-20140337940- A1 OR US- 20130191885-A1).did. AND PGPB.dbnm.)	(US-PGPUB)	OR	ON	ON	2024/03/09 06:59 PM
L53	24	("6757837" "6882712" "6889510" "7355730" "20020082924" "20060236325" "20070225828" "20080167127" "20080167128" "20080167133" "20090078760" "20100112997" "20100268401" "20110113087" "20110202798" "20110294466" "20120129492" "20120221893" "20120226619" "20120324067" "20140028449" "20140173059").pn. OR ("9129127").urpn. AND (PGPB USPT USOC).dbnm.	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM
L54	88	("6564056" "7664707" "7908401" "8311513" "8447696" "8974544" "9129127" "9141150" "9183380" "9204298" "9246921" "9489250"	(US-PGPUB; USPAT; USOCR)	OR	ON	ON	2024/03/09 06:59 PM

		"9507950" "9524174" "9531559" "9575477" "20040125782" "20050246243" "20080062258" "20080204199" "20090023395" "20100031371" "20100094981" "20110145927" "20130067551" "20130171981" "20130191885" "20130254437" "20130304795" "20130311684" "20140040989" "20140098247" "20140245765" "20140263612" "20140266669" "20140266679" "20140277597" "20140279109" "20140282486" "20140304632" "20140313048" "20140344454" "20140359042" "20140376528" "20150006686" "20150033305" "20150038129" "20150040246" "20150052578" "20150061859" "20150081928" "20150097689" "20150100618" "20150109104" "20150160935" "20150163412" "20150177705" "20150198938" "20150215337" "20150222578" "20150261954" "20150279134" "20150304171" "20150309548" "20150324179" "20150364028" "20160014108" "20160063854" "20160098362" "20160099972" "20160103494" "20160109864"				
--	--	--	--	--	--	--

L55	4	"20160119742" "20160142258" "20160142532" "20160294602" "20160337945" "20160351036" "20160380987" "20170019264" "20170034156" "20170034158" "20170046173" "20170048712" "20170078298" "20170093860" "20170099560" "20170109998").pn. OR ("10157271").urpn. AND (PGPB USPT USOC).dbnm. ((US-20170109998-A1 OR US-20170099560- A1 OR US- 20170093860-A1).did. AND PGPB.dbnm.) OR ((US-9575477-B2).did. AND USPT.dbnm.)	(US-PGPUB; USPAT)	OR	ON	ON	2024/03/09 07:00 PM
-----	---	---	-------------------	----	----	----	------------------------

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C	

U.S. PATENTS Remove						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	6101485	A	2000-08-08	Fortenberry et al.	
	2	7509487	B2	2009-03-24	Lu et al.	
	3	7844915	B2	2010-11-30	Platzer et al.	
	4	7975147	B1	2011-07-05	Qumei	
	5	8010669	B2	2011-08-30	Sathish	
	6	8195961	B2	2012-06-05	Ogawa	
	7	8370818	B2	2013-02-05	Osminer et al.	
	8	8406733	B2	2013-03-26	Raleigh	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C	

/	9	9032192	B2	2015-05-12	Frank	
	10	8620988		2013-12-31	Sohm	
	11	5581704		1996-12-03	Barbara	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/	1	20030096625	A1	2003-05-22	Lee et al.	
	2	20050207379	B2	2011-04-12	Shen et al.	
	3	20090037270	A1	2009-02-05	Patro	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/	1	1909463	EP	B1	2016-09-21	Hwang et al.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit			
	Examiner Name			
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C		

1	2	2006077283	WO	A1	2006-07-27	Houghton et al.		☐
2	3	2008048075	WO	A1	2008-04-24	Lee		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
1	1	"RDF Primer" W3C Recommendation 10 February 2004	☐
2	2	Baker, Loren, "Yahoo's RSS Reader goes LIVE on My Yahoo" January 26, 2004	☐
3	3	Cha, Bonnie, "Nokia E71 review: Nokia E71" July 2, 2008	☐
4	4	Dierks, T., "The Transport Layer Security (TLS) Protocol Version 1.1", April 2006	☐
5	5	ETSI TC AT-Features, "Work on MMS for PSTN/ISDN in AT-F" March 12, 2003	☐
6	6	Freier, Alan, et al, "The SSL Protocol Version 3.0", March 1996	☐
7	7	Global System for Mobile Communications; 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Function description; Stage 2 (Release 6) March 2005	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	
Examiner Name	
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C

8	Laplane, Phillip, "Dictionary of Computer Science, Engineering and Technology"; ISBN 0-8496-2691-5	☐
9	Miaj-E-Mostafa, "Transporting data between wireless applications using a messaging system -- MMS" July 7, 2006	☐
10	Open Mobile Alliance; "Enabler Release Definition for MMS Version 1.2" September 23, 2003	☐
11	Open Mobile Alliance; "Multimedia Messaging Service Architecture Overview Version 1.2" September 20, 2003	☐
12	IPR2024-00341: Petition for Inter Partes Review of United States Patent No. 8,406,733, filed on January 23, 2024	☐
13	IPR2024-00342: Petition for Inter Partes Review of United States Patent No. 8,406,733, filed on January 23, 2024	☐
14	File History of IPR2024-00341; filed on January 23, 2024	☐
15	File History of IPR2024-00342; filed on January 23, 2024	☐
16	Plaintiff Headwater Research LLC's Disclosure of Asserted Claims And Infringement Contentions, Headwater Research LLC v. Samsung Electronics Co., 6:23-cv-00103-JRG-RSP (WDTX)	☐
17	Plaintiff Headwater Research LLC's Amended Infringement Contentions, Headwater Research LLC v. Samsung Electronics Co., 6:23-cv-00103-JRG-RSP (WDTX)	☐
18		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C

	19		☐
--	----	--	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/FABRICIO R MURILLO GARCIA/	Date Considered	03/09/2024
--------------------	-----------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	
Examiner Name	
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

- ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

- ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-01-24
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Web Search History

date, time	web site	search string
3/9/2024 6:16:43 PM	Google Patents	Search Term 1 access networks wireless networks cable networks and DSL (Digital Subscriber Line) networks are pressed user capacity, EVDO (Evolution-Data Optimized) HSPA (High Speed Packet Access)
3/9/2024 6:16:54 PM	Google Patents	Search Term 1 networks cable networks and DSL (Digital Subscriber Line) networks are pressed user capacity, EVDO (Evolution-Data Optimized) HSPA (High Speed Packet Access)
3/9/2024 6:16:58 PM	Google Patents	Search Term 1 networks are pressed user capacity, EVDO (Evolution-Data Optimized) HSPA (High Speed Packet Access)
3/9/2024 6:17:01 PM	Google Patents	Search Term 1 EVDO (Evolution-Data Optimized) HSPA (High Speed Packet Access)
3/9/2024 6:17:17 PM	Google Patents	Search Term 1 HSPA (High Speed Packet Access)
3/9/2024 6:17:22 PM	Google Patents	Search Term 1 HSPA (High Speed Packet Access) LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access)
3/9/2024 6:17:27 PM	Google Patents	Search Term 1 Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access)
3/9/2024 6:17:31 PM	Google Patents	Search Term 1 (Worldwide Interoperability for Microwave Access)
3/9/2024 6:17:45 PM	Google Patents	Search Term 1 (increase new higher capacity wireless radio access technologies, such as MIMO)
3/9/2024 6:17:49 PM	Google Patents	Search Term 1 (wireless radio access technologies, such as MIMO)
3/9/2024 6:18:05 PM	Google Patents	Search Term 1 (higher average capacity per user, wire line user service consumption habits)

date, time	web site	search string
-------------------	-----------------	----------------------

3/9/2024 6:18:08 PM	Google Patents	Search Term 1 (wire line user service consumption habits)
---------------------	-------------------	--

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 July 2006 (27.07.2006)

PCT

(10) International Publication Number
WO 2006/077283 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) **H04Q 7/22** (2006.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/FI2006/050032

(22) International Filing Date: 19 January 2006 (19.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20050067 20 January 2005 (20.01.2005) FI

(71) Applicant (for all designated States except US): **STREAM MOBILE OY** [FI/FI]; Tammasaarenlaituri 3, FI-00180 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HOUGHTON, Paul** [US/FI]; Helmitäuluntie 13b, FI-02770 Espoo (FI).
REHTIJÄRVI, Pekka [FI/FI]; Itälahdenkatu 13 A 32, FI-00210 Helsinki (FI).

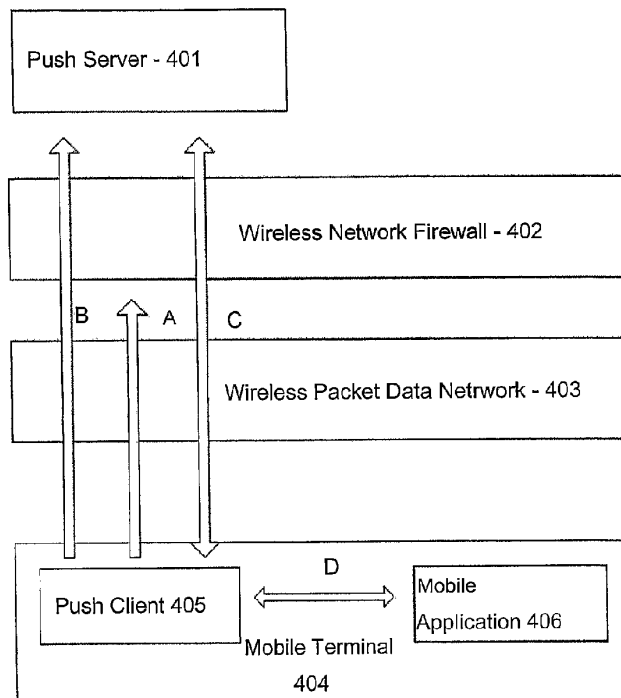
(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O. Box 148, FI-00121 Helsinki (FI).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PUSH MESSAGING COMMANDED METHODS AND DEVICES



(57) Abstract: A server outside a wireless network security entity is adapted to push messages to a mobile terminal located in the wireless network and thereby cause programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message thereby presenting a new application view to the user of the mobile terminal. The mobile terminal is provided with means, such as software, which initiates and maintains contact with the server using Internet technologies. This mobile-initiated permanent connection allows the server to pass or push messages from outside the operator's firewall to the mobile terminal at any time.

WO 2006/077283 A1

**Declarations under Rule 4.17:**

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *of inventorship (Rule 4.17(iv))*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *with international search report*

Title of the invention

Push Messaging Commanded Methods and Devices

Field of the invention

The invention relates to techniques for launching applications on a mobile terminal.

Description of the Related Art

The Internet is a collection of networks which exchange messages using IP protocol (Internet Protocol) and associated protocols which run on top of IP such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Gateways between IP networks automatically route and transmit information over primarily the IP4 and IP6 protocols between two or more end points on any of the connected fixed and mobile networks. Each of these networks may also include or run on top of other network transport protocols such as ATM (Asynchronous Transfer Mode) or a wireless protocol which in turn carry the IP packets over that section of the Internet.

Currently, the most common method of starting applications on a mobile terminal is to manually launch them by clicking on an icon or selecting a menu item. If the application, dynamically loaded program module or user interface feature is already launched, these applications must also be manually commanded by the user to change state to display newly available information provided by a telecommunications network. Some applications are also launched automatically when the terminal is started. This automatic start includes both applications that were installed on the phone before delivery to the customer including the basic terminal operating system software and programs installed by service providers and users and which by various means ask the terminal software to start them automatically after the terminal is powered up.

Remote launch to a known state as specified in a network command of programs on mobile terminals is supported in various telecommunications standards. Voice Over IP (VoIP) and other multimedia sessions can be started remotely using Session Initiation Protocol (SIP). Wireless Application Protocol Push (WAP Push) is another standard for launching programs on mobile terminals based on remote events. Java Mobile Information Device Profile (MIDP) and various native mobile terminal operating systems also support remote application launch based on receipt of a text message (Short Message Service,

SMS) or incoming Internet (IP) packet of information to a designated communications port number. However it is important to note from an economics and practical service deployment standpoint that each of these technologies either requires payment to the mobile network operator for sending an SMS or privileged access to the mobile phone from inside the operator's firewall in order for IP data to actually reach the phone.

Mobile phones and similar mobile communication devices were originally not permanently connected to the Internet. Instead, for the transmission and display of visual information they have relied on different telecommunications standards and proprietary communication systems such as SMS (Short Message Service, also known as text messaging) and MMS (Multimedia Message Service), which were built into mobile terminals.

Various techniques have been proposed for remotely commanding applications on a mobile terminal using push technologies:

US20020183051 relates to remote application management of a wireless device.

US20030208602 relates to pushing data in an internet protocol network environment.

US20010020255 relates to remote control and interaction with a mobile run time environment component.

US6687743 relates to client server communications for a mobile computing device.

US6779019 relates pushing information from a host to a mobile data communications device.

US6701378 relates pushing information from a host to a mobile data communications device.

US6463464 relates pushing information from a host to a mobile data communications device.

US6463463 relates pushing information from a host to a mobile data communications device.

US6389457 relates pushing information from a host to a mobile data communication device.

US2004122907 relates to secure interaction between a mobile client device and an enterprise application in a communication system.

WO0195695 discloses a system for wireless push and pull based services.

US2002187775 discloses a WAP service personalization, management and billing object oriented platform.

US2003106022 relates to outputting dynamic local content on mobile terminals.

US2004185834 discloses a method for enabling IP push capability to wireless devices on a wireless network.

US2002174184 shows a mailbox access mechanism using SMS push and WAP technologies on mobile terminals.

WO02077842 shows a push method for delivering data to mobile device.

Wireless Application Protocol Forum, Ltd., "Wireless Application Environment Specification, Version 2.0", Version 7-Feb-2002, 2002.

www.wapforum.org.

Sun Microsystems, Ltd., "The MIDP 2.0 Push Registry", Network and Timer MIDlet activation. developers.sun.com/techtopics/mobility/midp/articles.

Nokia, Ltd., "SIP Session Initiation Protocol", Forum Nokia 2005. www.forum.nokia.com/main/0,6566,1_44,00.html.

Nokia, Ltd., "SIP Frequently Asked Questions", Forum Nokia 2004. [SIP_FAQ_v1_0_en](#).

RFC 3261, "SIP: Session Initiation Protocol", 2002. www.faqs.org/rfcs/rfc3261.html.

Push technology is characterized by the server proactively sending documents or information to a client or user. E-mail (Electronic mail) is actually a special kind of push technology that has been prevalent for a long time. The first and most common general category of mobile content push technologies is SMS (Short Message Service) based technologies. SMS and MMS (Multimedia Messaging Service) are the most common forms of "push" messaging in the mobile industry. These store and forward messaging systems run by mobile telecommunications operators push all or part of the data to the mobile terminal over closed telecommunications signaling networks such as SS7 (Signaling System Seven). These signaling networks are closed; they are not part of the Internet. Each operator controls and encrypts this traffic, charging high prices for their use and limiting their use and usefulness.

FIG 1 shows a generic implementation known in the art for pushing launch and operational commands to applications on mobile terminals. Email, MMS, WAP (Wireless Application Protocol) pages, and custom application

data are delivered through existing telecommunications infrastructure to a mobile terminal using SMS as the push messenger medium. First, push server software 101 delivers the notification to an SMS Gateway 102, as illustrated by the arrow A. The SMS Gateway puts the actual SMS push message in either readable text or compressed binary format into the telecommunications signaling network 103, usually SS7, which delivers it in a store and forward fashion often involving several intermediate steps to the mobile terminal 104, as illustrated by the arrow B. The mobile terminal standard software 105 decodes header information in the SMS and based on the fields in this binary SMS header not visible to end users, delivers this as a normal SMS, an MMS, WAP pages or a custom application command action (C) to the indicated mobile application 106, launching the application if necessary. These custom application launches by SMS require the application to first register itself with the mobile terminal in order to receive SMS push message command events.

Besides a high price per message, SMS messages cost different amounts depending on where the sender and receiver are located. In some countries the sender pays for the message, in other countries the receiver pays. Computers called Short Message Service Center (SMS-C) nodes and owned and managed by each mobile operator deliver SMS messages. In many cases, if the sender and receiver are on different continents the operators do not even offer message delivery. Two operators must negotiate, sign and implement a legal contract known as an interconnect agreement before messages flow between SMS-Cs and thus between mobile terminals on different operator networks. Since not all operators have such contracts with all other operators, this limited connectivity also means that commanding mobile applications based on any SMS technologies can not be delivered on a global basis. For example an SMS-based remote application command server run from a European telecommunications operator will face the practical limits of incomplete operator interconnect agreements when pushing application commands to their North American and Asian customers. Also, because of the billing models in different countries are also variable, high costs and delays when roaming, it is difficult to develop reliable global application command using SMS-technologies. For example, such SMS delivery arrangements to all operators within one country or in multiple countries usually rely on expensive arrangements with middlemen or brokers that route computer-originated mes-

sages to phones in many locations. Even the best of these such middlemen still do not offer global coverage to all countries.

A newer telephone company standards-based method to delivery content and command applications which have not been explicitly requested by the user of a mobile terminal is WAP Push. WAP Push technology relies on an SMS to start the message delivery process. Both SMS and WAP Push using SMS can be used to command applications on the phone. Java applications on mobile terminals can also register themselves to be launched upon receipt of an SMS and then interpret the contents of the SMS as a type of launch command or launch content. But in all these cases operators continue to control the push medium and charge money for each push event. This operator control of content on mobile terminals is known in the industry as the "walled garden" approach.

SMS messaging standards include the ability to send binary messages to an application installed on the mobile terminal. Parameters in the message header and applications in the mobile terminal are matched by the mobile terminal at delivery time and the selected application receives the pushed SMS contents, starting the application if it is not already running. This is a standard software feature installed on the phone at time of manufacture as part of the mobile terminal's operating system.

The cost of using such an remote command capability is quite high—the cost of an SMS each time the program is commanded, thereby limiting the broad utility of this feature for all but a telecommunications operator supplying the service only to their own customers. These standard SMS-based telecommunications technologies for push application remote command are all thus limited by economics in both the frequency with which they can be used and the breadth of market which they can reach. Also due to the low speed of SMS delivery as a store-and-forward messaging system, it can take a long time for the application to launch to a known state based on a remote command thus making this unsuitable for use in any real time or time critical situations.

A further limitation of existing SMS remote command technologies is the inability to prioritize, select and deliver messages in different ways to a user based on their current situation, location and individual preferences. More important application command events may be buried behind several less important events causing critical items to be missed or confused. A user can not select with these SMS-technologies not to be notified, or to be notified in a

more polite manner, or to go ahead and start to a known state or change the visible operating state of the application without politely asking in some circumstances. And a user can not specify that they would like to only receive or receive a request for permission to execute a certain category of application command events during a given period of time.

A second general category of mobile push technologies is IP-based technologies. These include IP connections initiated from the server and IP connections initiated from the client. Server-initiated push connections are the most commonly described. These solutions require IP communication with software installed on the terminal and a server which has been notified of the IP address of this terminal. The server then, when a push event is desired, initiates a connection to the terminal and delivers information to it which software in the mobile terminal can then act upon, most commonly to notify the client of an incoming email message. For reasons described below, these push technologies are not generally used on mobile terminals but are more commonly used between one server and another as in the SMTP mail transport protocol when delivering email. Similar methods are also used for launching, commanding and communicating with applications on servers and in some cases on mobile terminals.

There are, however, difficulties with commanding applications on mobile terminals based on receipts of an IP packet when there is not an already established IP connection between a mobile application program module or feature and the command push server. In practice, mobile terminals are on sections of the Internet which are most commonly behind a firewall or gateway server device creating a controlled mobile network. This difference from the above-mentioned server-to-server push technologies is non-obvious when reading standards and results in many server-to-client and server-to-mobile-terminal push technologies which in practice do not work because of firewalls protecting the mobile terminal. Thus firewall and mobile gateway devices at the connection between the security-controlled mobile network and the more public Internet frequently restrict computing devices such as servers on the public Internet from directly contacting mobile terminals. Additionally, IP connection and security techniques, such as network address translation, firewalls and gateways, may hide the actual address of the mobile terminal further complicating direct connection from an Internet computing device. Further, the mobile

terminal may be unavailable at any given time making such messages undeliverable.

The public telecommunications operator, company, organization, or private individual setting up a mobile Internet space with one or more users uses the above-mentioned firewalls, security devices and gateways to protect the mobile terminals from hostile or unwanted contact common on the public Internet. They may also do so to reduce background traffic, protect their control over this space and thereby limit outside or undesired service providers through technical connection policies set in the firewall or gateway device. The result is, if a fixed or mobile computing device from outside the controlled mobile network tries to contact a mobile terminal inside the controlled mobile network, the connection is not permitted unless the organization or individual controlling the firewall or gateway server device makes an exception to their security policy and explicitly allows the connection. Instead, in standards-based mobile Internet telecommunications, an intermediary computer with privileged access from inside the firewall to the mobile terminals is used. These server computers such as a telecommunications operator SIP Server or WAP Gateway is used to control and deliver messages and store messages when the mobile terminal is unavailable and deliver them on the senders behalf, possibly later then the terminal becomes available, or to forward them to a different gateway device, for example if the user is roaming to a different controlled mobile network.

The most common solutions to accessing mobile terminals subject to this mobile network restriction are to either make an agreement with the public or private network operator removing the security restriction on a specific outside server contacting mobile terminals, or to move the server inside the controlled network. In the common case of a public mobile network operator, the state of the art and most common solution is to sell the server and associated software to the mobile operator so that they can provide the service to their customers. Both of these solutions require time, effort and often large financial commitments. And they must be done for each and every restricted mobile network and operator in a given market to achieve universal access to a service requiring server-initiated IP push. Achieving such universal penetrations on all operators in all markets is not practical. However for those operators with whom such a relationship has been established, mobile application launch and command with standard IP technologies is thus possible.

Client-initiated mobile IP connections are less common in mobile terminals. These are also not part of state of the art mobile application command telecommunications standards. Client-initiated IP connections involve installing more complex software on each mobile terminal and having these devices initiate contact to a server on the public Internet. These connections generally operate in a polling or "content pull" manner, connecting intermittently to the server to ask if any new information is available. Mobile email is a common example of this approach for content download. While the result appears to be push to the end user when they are notified several minutes later of the incoming email, they were not notified immediately by the server when the message is available as in true push technologies. The network settings of the mobile terminal may also need to be adjusted to permit this since Internet access through default gateway devices may not permit this type of connection.

FIG 2 shows a generic implementation known in the art for pushing launch and operational commands to applications on mobile terminals using Internet technologies. Symbian, Linux, Microsoft and other mobile IP terminal operating system software all include application launch capabilities based on this socket-based triggering mechanism. Each mobile application 205 has a fixed IP port number such as TCP/IP or UDP/IP port numbers. When a remote program such as a push server 202 sitting inside the operator's firewall 201 and with permission to contact ports on the mobile terminal 203 sends an IP packet to the terminal (A), the IP terminal software 204 routes the packet with it's commands or application-specific data to the mobile application 205 (B), launching the application if it is not already running. Java applications sitting on top of the lower levels of IP terminal software can be similarly launched based on Java MIDP 2.0 and later "push registry" settings.

FIG 3 shows the same steps A and B shown in FIG 2, however the push server 301 may be located outside the firewall 302 because the wireless network firewall has been configured by the mobile network operator to allow communications from that particular push server. This allows IP traffic to flow from the push server 301 to the IP terminal 303 and be internally routed 304 to the mobile application 305.

The important point to note in the standard methods shown in both FIG 2 and FIG 3 is that the permission of the wireless network operator is required to either locate a push server within their firewall or open a firewall hole to a given push server. This permission is in practice expensive for an arbitrary

push server to achieve with a given operator. It is virtually impossible to achieve with all mobile network operators in all markets. A viable market alternative to the state of the art methods shown in FIGURES 1, 2 and 3 for the mobile terminal and push server to initiate and maintain contact for push application launch and configuration commands without explicit arrangements with each mobile network operator is thus needed and described in the invention below.

Once such an IP connection is established between the server and one or more mobile terminals, the connection can be used to transfer messages to the mobile terminal. The most interesting such messages for the present invention are event trigger messages to launch or command a mobile application. Other interesting uses include the sending of data files, new applications and applications updates to replace or improve installed applications. These messages, while simply inexpensive IP traffic can if sufficient in number result in significant costs or the user perception of their incurring significant data traffic costs. For this reason it is also desirable to route such information including application updates, bug fixes, additional features, additional application data including multimedia, vector graphics, text and executable code through the lowest cost available network connection. Further it is desirable but not generally possible to automatically do so only during those times that a lower cost network connection is available as through the presence of a broadband wireless access device.

Numerous mobile applications such as games and productivity software are now included with new mobile terminals. They can be used to perform an endless variety of tasks, some of which involve interaction with elements outside the mobile terminal, for example on desktop computers, servers and other mobile terminals which are also connected to the Internet. The process of a user manually performing actions such as starting the mobile application to become aware of the state of remote computers and terminals is referred to as pull because a user action triggers or "pulls" the information for display to the phone.

Multimedia audio and video presentation applications, Voice over IP (VoIP) communications, multimedia interaction applications, games including games which involve other player and automated server actions such as game events and challenges from other mobile terminals, mobile business process applications, real time back office connectivity applications and corporate mes-

saging programs are examples of areas where mobile terminal applications benefit from the ability of server placed arbitrarily on the public Internet having the ability to initiate the display of or remotely configure the view presented by an already running program on a mobile terminal at any time. Due to technical limitations of the terminal and user preferences, it is generally not possible for a mobile terminal to support multiple such large or resource-intensive applications running continuously. Therefore there is a need for a more general solution to automatically install, update, provide data to, launch and configure these applications from the background on mobile terminals on any mobile network.

Commanding an application on the mobile terminal, launching an application with parameters specified in the launch message so as to view specific information after the program starts, changing the current view of an application which is already running, pushing or pulling new information into an application so as to change what is presented to the user are all referred to herein as changing the state of the application. This application state change process generally requires personal initiative and several manual and cumbersome steps and decisions on the part of the user: opening the application or changing the view of the application, selecting and then examining the content to see if any of the changes are of interest. Because of the limited size, network bandwidth and user interface of mobile terminals, performing these steps is significantly slower on a mobile terminal than performing the same actions on a larger computer. The process of checking if an application should be launched now because new and interesting Internet information might be available is therefore less interesting to mobile terminal users than on a larger terminal because of the limited capabilities of the mobile terminal to rapidly display many alternative content formats. This frustrating or slow user interface with for example small buttons, touch screen or relatively slow interface response on the mobile terminal is one of the reasons there is commercial need for eliminating the user steps and push commanding the mobile application remotely from a server only when new and interesting information is available.

Given the shortcomings in the prior art, there is a need for a method whereby a computer on the Internet can rapidly and at reasonable cost be permitted to at any time initiate control of one or more applications on an individual's mobile terminal to deliver through that mobile application real time in-

formation, interactivity and rich media content, regardless of which mobile operator is being used and where the mobile user happens to be at that moment.

Brief description of the invention

An object of the present invention is a new technique for providing a push-type command of applications on a mobile terminal by a remote server computer. The object is achieved by the invention is characterized by what is stated in the attached independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

In a preferred embodiment of the present invention is a system and method for a server placed freely on a connected network outside the wireless network firewall or other corresponding wireless network security entity, to push messages to a mobile terminal located in the wireless network and thereby cause programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message thereby presenting a new application view to the user of the mobile terminal. The mobile terminal is provided with means, such as software, which initiates and maintains contact with the server using Internet technologies, thereby avoiding cost, latency, contractual and firewall penetration issues of the server contacting the mobile terminals by telecommunications messaging or Internet technologies. This mobile-initiated permanent IP connection allows the server to pass or push messages from outside the operator's firewall to the mobile terminal at any time. If the server would attempt to use IP to contact the mobile device directly, the attempt would fail due to the firewall(s).

In an embodiment of the invention, the mobile terminal maintains contact with the server by periodically testing the connection with a suitable keepalive message, a "ping", which resets timers in intervening operator stateful firewalls and/or NAT (network address translation) firewalls. The mobile terminal may also automatically re-establish the connection when the connection gets broken and adjust its connection settings based on past experience with failure to connect and such broken connections in a given mobile network.

In an embodiment of the invention, the push messages may include, for example, a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface feature of the terminal such as an application which is part of the basic terminal software or and an additional installed application beyond the base software supplied with the mobile termi-

nal. In response to receiving such a message, a mobile terminal may spontaneously open the application, dynamically loaded module or user interface feature of the terminal thereof to a designed application view or location, present new information of the availability of new information, a new feature or operating state. If such application, module or user interface features is already operating in the mobile terminal, the action of such a message would instead stimulate the application or user interface feature to present itself to the foreground of the user interface and change state as specified in the application-specific message received from the server. In further embodiments of the invention, push messages may include, for example, messages triggering the mobile terminal to play a sound notifying the recipient of the application command or state change, or display notification providing event information from which the user may select or decline to display the application.

Note that in some cases the packaging of mobile applications involves combining multiple applications delivered in a single bundle or application suite preinstalled or later installed to the mobile terminal. Commanding the display of an additional, more resource-intensive user interface feature such a rich media, or highly interactivity modes within the same bundle of applications or application features as for example by explicitly or implicitly loading or calling an additional library such as a user-interface related code or other embodiment of an application on a mobile terminal within the same application based on push event messages recently received from an IP connection is simply an alternative packaging of this same invention. For brevity herein, this type of commanding of a new user interface modes or view to appear within the same application suite is considered and discussed as the commanding of a new application since the packaging of rich user interface features and program modules within a bundle or separately is a relatively minor detail in the embodiment of the invention.

The cost for a user's mobile terminal to maintain a connection to the push server and receive such messages over mobile Internet connections is minimal, thereby solving the problem of some mobile information services not being economic to offer. The advantages are: all the convenience of standard push services such as SMS-based application launch and command together with the mobile network-independent and economic benefits of placing the server outside of any single operator's network and of the service provider not having to pay an operator or operator middleman per command event.

IP push messages utilizing the principles of the invention are delivered rapidly, bypassing the public and often crowded SMS, MMS, WAP Push and email store-and-forward mechanism within an operator and between operators. This guarantee of very rapid event push provides usability benefits to users which may be then designed into the mobile applications. For example the ability to expect prompt delivery allows modification to interactive mobile application system design. The mobile process surrounding the application can be changed such that a user on one mobile terminal may take actions which result in the initiation of a push event to a user on a second terminal and then wait for a short time for the second user to respond after the launching or commanding to return to be the focus of user interface attention their copy of the same, similar or complimentary mobile application function involving Internet communication directly or mediated by a server between the two mobile applications.

The advantages of performing push service application command in accordance with the present invention include the ability to run such a service from outside the mobile operator's firewall and gateway devices, skip the overhead charges like per-message SMS fees normally associated with "mobile push", and make it easy to create mobile applications as web pages, therefore usually without programming. Thus, push application command services according to the invention can be modified from existing or newly designed mobile applications, modules and application features simply by creating an application command, module or feature entry point compatible with the embodiment of the push client. This embodiment can be, but is not limited to, a separate application, operating system background process or application module bundled in a suite with the mobile application and kept running such that it may receive IP push events and command applications, modules or significant application features.

These messages may be routed automatically to a nearby computing device with faster or less expensive network connectivity such as a broadband access point, server or workstation in the proximity of the mobile terminal. Both mobile terminal and access point must be equipped with a wireless communication network such as RFID, Bluetooth, ultrawideband, Zigbee, Wi-Fi, Wi-Max or other personal area, local area, metropolitan area or large area network. This ability embodied in the invention alleviates speed and economic problems that affects the present-day mobile messaging solutions which are either limited in bandwidth or cost based on volume of use. When in proximity to a more

capable network, if a connection can be established to this alternative broadband network access point, it is used preferentially and intelligence normally located in this broadband access point would route messages received on behalf of the wireless terminal to and from the server. Further, the availability of a broadband access point would be notified to mobile terminal application software and server alike allowing either to initiate bandwidth intensive operations such as application update and application data update.

IP push command messages may be triggered either by events which the server is aware of, or events which a similar mobile application on another mobile terminal is aware of and which that push client makes the server aware of, the server in turn initiating a push command event. Such client-side events of which the server is informed for the possibility of delivering new web services include the making, receiving, and termination of telephone calls, the transition from presence-to-absence or absence-to-presence of other devices in a geographical area, metropolitan area, local area or personal area wireless communications network, mobile terminal creation of photographs video audio or other media, mobile terminal presence of files matching a given filtering criteria, changes in internal state of electronic equipment, taking of measurements, processing of such measurements to see if they match certain criteria, video game actions or events, application calculation events and messaging actions. In some cases a separate server such as a telecommunication service server, gaming environment server, and original equipment manufacturer device or business information system may notify the server directly of events or messages to be sent using an external application programming interface (API). Such a device connected by external API may also receive information including the results and responses of messages which the user has replied to by terminal software or web page interaction.

The invention provides content and application producers with a cost effective, network-independent and device-independent service for the rapid creation and distribution of interactive information alerts and Internet launch-at-will and present-when-needed features for their users.

The invention provides techniques for launching and changing the operating state such as information currently presented to the user of applications on a mobile terminal at will by a server computer and without the need for any additional action by the recipient, and more specifically to a system, method and program for sending, receiving and acting upon messages sent to a mo-

mobile client device over a packet switched data network for the purpose of initiating application launch, application command, module or feature display and user direct or indirect user interface state change based on server-side events and mobile terminal events including user interface events, phone calls and network proximity events, and local resource changes.

Brief description of the drawings

In the following description, reference is made to the accompanying drawings which form a part hereof, and which illustrate several embodiments of the present invention. In the drawings:

Figure 1 shows an implementation known in the art for pushing information including commands to an application through existing telecommunications SMS infrastructure to a mobile terminal and if necessary launching the application;

Figure 2 shows an implementation known in the art for pushing information including commands from inside the mobile network firewall to an application to a mobile terminal and if necessary launching the application;

Figure 3 shows an implementation known in the art for pushing information including commands from outside the mobile network firewall through a firewall hole opened by the mobile network operator to an application to a mobile terminal and if necessary launching the application;

Figure 4 is a block diagram illustrating an exemplary implementation of the system for pushing mobile application launch commands to a mobile terminal based on server side events in accordance with one embodiment of the present invention;

Figure 5 is a block diagram illustrating an exemplary implementation of the system for a wire terminal with an alternative broadband connection to use the alternative broadband access point for receiving push messages including launch events, application updates and data updates;

Figure 6 is a flow chart illustrating an exemplary process by which the mobile terminal maintains an open path for network communication with the server (6A), keeps the connection to the server open and tests the integrity of the connection while automatically reestablishing the connection as necessary (6B), responds to messages from the server (6C), and notifies the server of locally monitored events on the mobile terminal (6D) in accordance with one embodiment of the present invention;

Figure 7 illustrates an example of a "COMMAND PUSH" procedure;

Figure 8 illustrates an example of a "COMMAND PUSH WITH BIDIRECTIONAL DATA" procedure;

Figure 9 illustrates an example of a "BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA" procedure;

Figures 10A, 10B and 10C are flow diagrams showing examples of processes by which the server maintains a connection with the client and communicates commands and data to it.

Detailed Description of the Invention

In the above description, the invention is described using various embodiments of the present invention as examples but the invention is not intended to be restricted to these embodiments. It is understood that other embodiments may be utilized and structural and operational changes may be made without departing from the scope of the present invention.

Figure 4 illustrates an exemplary implementation of the system for pushing application commands to a mobile terminal based on server side and client side events in accordance with one embodiment of the present invention. More specifically, Figure 4 illustrates a Push Client basic functionality 405 implemented in a mobile terminal 404 as part of a message passing system in cooperation with a Push Server 401. The push client 405 is preferably implemented in the form of a software run in a processor of the mobile terminal 404. The mobile terminal 404 is preferably a commercially available mobile terminal, such as a portable phone or appliance capable of running software or personal digital assistant, which provides a platform for downloading application software over air or from a personal computer, installing the software in the terminal, and running the software in the terminal. For example, the Symbian operating system is an open operating system, application framework, and application suite optimised for the needs of wireless information devices such as intelligent phones, smartphones and communicators, and open operating system and drives standards for the interoperation of data-enabled mobile phones with mobile networks, content applications, and services. The Symbian operating system also includes connectivity software for synchronisation with data on personal computers and servers. The application may be in an appropriate programming language, such as C++ or Java, which is an object-oriented pro-

gramming language and virtual machine platform developed by Sun Microsystems.

The push client software 405 preferably launches automatically when the mobile terminal 404 is turned on. The push client software 405 runs in the background and attempts to log into the push server 401 over a data network 403, normally a wireless network capable of transmitting Internet Protocol (IP) packets. The arrow A in Figure 4 illustrates an optional attempt by the push client 405 to communicate with the wireless network firewall 402 or other similar security or gateway device in order to open a connection for the push server 401 to directly contact the push client 401 as in FIG 3. If successful, operations can continue as described in FIG 3 or as below. Arrow B illustrates a login attempt.

The wireless network 403 may be protected by means of a firewall or other appropriate security entity 402, which connects the wireless network to the public networks and filters and selectively discards the data packets entering and exiting the wireless network according to predefined rules. Thus, a firewall is a gateway device which operates at the same time as a connector and a separator between networks in a sense that it keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Additionally, IP connection techniques, such as Internet Protocol 4 (IP4) network address translation and Internet Protocol 6 (IP6) security, encryption and/or authentication, may hide the actual address of the mobile terminal or make it otherwise difficult for a server to connect to directly to the mobile terminal. The public telecommunications operator, company, organization, or private individual setting up this mobile Internet space with one or more users having greater ability to contact one another and included servers does this to protect the mobile terminals from hostile or unwanted contact common on the public Internet. They may also do so to reduce background traffic, protect their control over this space and limit outside or undesired service providers through technical connection policies set in the firewall, gateway or other security device. Physically a firewall may be a machine with appropriate software to do the task assigned to it. 402 can be a firewall, router, a personal computer, a gateway server or whatever similar computing device, infrastructure or secure protocol such as IP6 can be used for such purposes.

Consequently to the existence and configuration of 402, if a fixed or mobile computing device from outside the controlled mobile network tries to contact a mobile terminal 404 inside the controlled mobile network, the incoming connection is not generally permitted unless the organization or individual controlling the firewall, gateway server or security device 24 makes an adjustment to their security policy and explicitly allows the connection.

From point of view of the wireless packet data network 23, the login attempt B and associated connection establishment C is one or more normal IP connections established at the request of the mobile terminal. If optional attempt A to open a path for the push server 401 to initiate the IP connection now or in the future, use from that point forward may proceed as in FIG 3. However this firewall and/or security device or protocol opening A is unsuccessful, the login attempt B is in either case normally allowed to pass the firewall or security infrastructure 402 since the connection is from the inside the firewall to outside.

After attempting login, if the login is not successful the client 405 may automatically or under supervision of the user of the mobile terminal 404 try several different techniques for contacting the server 401. Since there are numerous variations between mobile terminals and in network connectivity, more than one connection attempt may be needed to contact the push server 401. Differences in wireless network terminal characteristics, individual push server availability and accessibility, firewall and gateway permissions, connection timeouts, connection level stateful (such as TCP) and stateless (such as UDP) transport protocol availability (such as IP4, IP6, SSL, HTTP, HTTPS) and alternate mobile terminal network settings mean that a sequence of connection establishment attempts and connection maintaining steps may required to be made using variations in relevant network parameters.

A second reason for automatically adjusting the network parameters is not simply establishing the connection but establishing the connection in the most cost effective or highest performance configuration available for the individual mobile terminal user account service level. Connection types differ in speed, customer expensive, server resource usage and hence scalability, security and ability to penetrate gateway security devices. Some customers may be offered more secure or higher performance service while others receive the least cost connectivity from either the mobile terminal's or the push server's standpoint.

As an example, such network parameters may include but are not limited to one or more of the following:

- Use of a connection-oriented protocol suitable to the wireless network such as TCP/IP protocol, which is generally preferred in the common situation where an intermediate firewall, Network Address Translation (NAT) or gateway device 402.

- Use of a connectionless protocol suitable to the wireless network 403, such as UDP/IP, which is generally preferred when no network device restricting terminal contact 402 is present as this reduces resource usage on the server when large number of mobile terminals is served.

- Use of an alternate connection-oriented protocol such as HTTP suitable for mobile push operation through more strict firewalls and proxy Internet connections.

- Use of a secure protocol such as HTTPS, IP-Sec, secure IP6 or a proprietary security protocol to identify the communicating parties, prevent message interception by 3rd parties, and prevent message modification by 3rd parties.

- Use of a periodic message from the client to the server or server to the client to the effect that client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices do not time expire the connection.

- Use of configuration messages to the firewall (FIG 4, A) using a firewall or other security configuration protocol, such as Universal Plug and Play, to open a path for server-initiated connection-oriented or connectionless messaging to the client.

- Use of periodic messages initiated by the client 405 or by the server 401 to the effect that the receiving application is informed that their messages are continuing to be received, as indicated by response data from the receiving party to the sending party.

- Use of longer or shorter timing between such periodic messages to match the combined needs of all such network devices and protocols involved in transmitting communication, as adjusted based on the success or failure of earlier messages to successfully traverse the open network connection.

- Use of an alternate push server network address such as an address accessible with fewer security and performance restrictions which may be more available, more accessible, lower cost, lower latency, less busy, higher

bandwidth or otherwise preferred at the present time and from the present network location of mobile terminal 404.

- Use of one or more alternative mobile terminal network connection settings, or variation of the parameters within the settings.
- Use of an alternate connection route through a second mobile or fixed terminal accessible to the mobile terminal over an alternate wireless network or network connection and capable of communication with a push server.

In an embodiment of the invention, the mobile terminal 404 keeps a prioritized data structure listing the preferred communication protocols, server addresses, periodic message timings, network access settings, and alternate communication routes which it should use. Automated and manually assisted use of this structure should then result in a connection to one or more push servers, however if one of these connections which the mobile terminal is programmed to expect is not available, the mobile terminal can choose the sleep that function of the client software and attempt re-connection at a later time, repeating in like fashion with the same or different network connection parameters as described above until a connection is established or other user intervention.

At any time after a connection is established between the client 405 and the server 401, the client may push a message to the server or the server may send a push message to the client. This is illustrated by means of the arrow C in Figure 4. These messages through a previously established, connection-oriented protocol such as TCP/IP, SSL, HTTP or HTTPS arrive quite rapidly, more rapidly than if the connection were established only when needed. The associated protocol overhead such as 3-way handshake during connection establishment thus occurs before the actual need for message transmission rather than needing to occur at time of transmission and thus delaying the transmission.

A connectionless protocol, such as UDP/IP, may also be used in cases where the connection-oriented protocol is not possible or not desirable because of the push server resources used by every static instance of a connection-oriented protocol. Connectionless communication is also used when a message needs to get through to the server 401 quickly, such as when occurs when the client 405 notifies the server 401 of a terminal event, user interface event or application event but the connection-oriented protocol connection is not connected or is already busy transferring information. Such a selective use

of this high priority, low latency communication channel from terminal 404 to server 401 gives the server the opportunity to in return push to the client 405 a service triggered by the event begin communicated by the client 405 as will be described in more detail below. The sending of such a return message is frequently time critical and the fastest available combination of techniques will be used.

In the preferred embodiment of the invention, the most basic message pushed from the server 401 to the client 405 is a data packet containing no information. Additional binary or text information specifying which mobile application 406 from a plurality of such applications may optionally be included. Additional binary or text information to be passed to the default or specified mobile application may optionally be included. Additional binary or text information specifying how upon receiving such a message the client 405 will notify and optionally ask the user if the action should be performed may optionally be included. Upon receiving such a message, appropriate automated actions and user interface media capabilities of the mobile terminal as specified in the command C from the server 401 are executed by the push client 405. The most common case is playing a sound, asking the user if the mobile application should be launched, and if affirmative passing the command details (arrow D) to the specified mobile application, module or additional feature within the same application suite, launching the application, module or feature if needed. Such action may include optionally proceed without audio, with network downloaded audio, or without first requesting confirmation from the user as specified by user preferences and command details.

The push message from the push server 401 may be triggered by any trigger event, local or remote, defined at the server. The trigger may, among others, include an alarm, notification, or measurement result received to the push server 401 from another device or system. With a push message, the server 401 may direct the mobile application 406 to make use of additional network resources either on the push server or other server. The push client 405 may in turn at any time accept data D from each of a plurality of mobile applications 406 and direct such to the push server 401, possibly for redirection through push server API to other servers, mobile terminals, push clients and computing devices.

Figure 7 illustrates an example of an "COMMAND PUSH" procedure wherein the push server 701 is triggered by a trigger event as for example from

an application server 702 to push an application command message to the push client 704 and thereby initiate a mobile terminal client trigger event in a mobile application 705 from a plurality of such applications, program modules and user interface features on the terminal 705. The trigger event from push client 704 to mobile application 705 may optionally include commands or data affecting the aspect of visual presentation of mobile application 705. The even trigger mechanism may be any electronic process mechanism as for example computer software calls to load or configure a class, library, dynamic link library, MIDlet, Symbian application, Linux daemon or other executable object. The trigger mechanism may be between separate parts of a larger application or application suite, or may be an IP-triggered application launch and data transfer as in the case of mobile application launched by contact to a specified IP port. The potential applications of the COMMAND PUSH include but are not limited to mobile applications for enterprise connectivity, back office integration, database access, scientific and industrial process and equipment monitoring and control, pictures transfer, mobile gaming, application data transfer, mobile electronic commerce, application alarms, reminders, multimedia interactivity, corporate calendaring, personal messaging and group messaging, etc.

The push server 701 may in combination with user preferences stored in either the push server 701 or push client 704, optionally request the push client 704 to display or otherwise as appropriate for the mobile terminal or appliance notify the user asking permission for launching mobile application 705 prior to application launch. The preferred embodiment is for the behavior, language and content of this information to be configured on the server 701 based on the service and preferences of the individual receiving the message. In such cases an optional informational message will be presented to the user and such information messages are associated for instance with the menu option transmitted to the client 704 by the server 701.

In an embodiment of the invention, the client 704 is also capable of receiving and storing variables which configure behavior of the client 704. The server 701 may thus specify the network connection preferences, notification sounds, and other behavior of the client 704. These changes facilitate the efficient and manageable operation of the entire system and can be used for automated remote maintenance of push client 704, mobile applications as 705, and configurable aspects of underlying mobile terminal 703, for example

changing the username, password, and security certificates stored in the mobile terminal.

Figure 8 illustrates an extension of the procedure in Figure 7, one known as "COMMAND PUSH WITH BIDIRECTIONAL DATA". This embodiment of the invention includes all aspects of "COMMAND PUSH" with the additional step that a data connection between application server 802 and mobile application 805 is established with the aid of the persistent managed, tested and configured data connection in Figure 4, arrow C between push server 401/801 and push client 405/804. An IP or other API (application programming interface) connection between application server 802 and push server 801 simplifies the work and cost of creating application server 802 by taking care of network details already established for the COMMAND PUSH procedure. Similarly, an IP or API connection between push client 804 and mobile application 805 completes the connection and reduces the number, cost and resource usage of a possible plurality of such connections for a corresponding plurality of mobile applications. Further, each mobile application 805 is now free to sleep, exit or otherwise release the limited resources of the mobile terminal 803 with the assurance it may be remotely commanded back into action provided at least one push client 804 from a possible plurality of such push clients remains active, connected to the push server 801 and configured to launch the mobile applications 805.

Referring now to Figure 5, users of mobile terminals 507 are frequently but not continuously in range of alternative and more desirable wireless network access (Figure 5, arrow A). Such access is shown in the exemplary embodiment as broadband access point 509 within alternate and more desirable for reasons such as speed, cost and security broadband wireless network 507. Such an access point 509, which may also be mobile, is referred to herein as a broadband access terminal. The push client network connection functionality according to the invention may also be installed on such a broadband access point to facilitate routing and connection over alternative wireless network 507 such as a bluetooth, Wi-Fi, Wi-Max, Zigbee, radio frequency, infrared, ultrawideband, grid network or similar opportunistic or ad-hoc wireless network. Thus, both devices 508 and 509 have the minimal capabilities of client software 405 necessary for establishing and maintaining the already established contact with push server 501. Further, the two devices detect one another and so noting inform the server 501 through connections B or C and are thereafter

temporarily associated with one another in the server for routing and mobile application launch and data transfer purposes. Further, the push server 501 on becoming aware of such a situation may inform (arrow D) the application server 502 of the availability of a more desirable network connection (C plus A) to the client and on behalf of the application server 502 or independently decide to push additional commands and data to the wireless terminal using this connection. Further, the push client in the broadband access point has the additional capability to route such information to the wireless terminal. The result benefits customers using the wireless terminal in that data is managed and updated automatically for their mobile applications in the most cost efficient manner for non-time-critical capabilities such as lazy application code update and lazy application data update. While such alternative routing may also be achieved through normal IP routing and path cost without the presence in the broadband access point 509 of push-aware client software, the push server 501 and application server 502 would in this known-in-the-art implementation not be aware of when the low cost alternative route was available and thus able to at such time trigger the push of lazy application code and data installation and updates.

Figure 9 illustrates an example of a "BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA" extending the earlier discussed "COMMAND PUSH WITH BIDIRECTIONAL DATA" disclosed in Figure 8. This procedure wherein the push server 901 has been earlier informed by either the mobile terminal push client 906 or broadband access point 904 of the available alternative broadband network 507 and associated route (Figure 5 D, C and A, corresponding to Figure 9 A, B and C). Based on this notification and user preferences the push server 901 may choose to route future messages to either device, however the preferred remote application command push and data route is indicated by arrows B and C. Then at some later time the push server 901 is triggered by a trigger event of which the application server 902 is aware to send push message to the mobile terminal 905, and procedure steps A, B, C are traversed thereby pushing application launch commands, lazy application updates, and lazy application data updates through push clients 904 and 905 to mobile application 907 through local command and data path D (also Figure 5, arrow A).

Figures 6A, 6B, 6C and 6D are flow diagrams showing examples of processes of the preferred embodiment by which the client 405 maintains a connection with the server 401 and communicates messages to it.

Firstly, in step 602 the push client 405 initiates an attempts to log into the push server 401 over data network 403, as indicated by the arrow B in Figure 4. Success of the connection attempt is monitored in step 603, and if the network connection shows an error or does not get a response from the server in a reasonably short time the network settings are adjusted in 604 (for example in the manner describe above if the network connection fails). If the server does connect but login fails at 605, the push client may change the login settings in step 606 (for example in the manner described above if the login is rejected) and retry the login. If the login to the push server 401 is successful, a connection is already opened to the client 405 and the application server 405 changes state informing applications server 502 from a plurality of such server of the availability of the client 401 and relevant details. Thereafter the mobile applications 406 of a plurality of such applications can be contacted until the server 401 is otherwise notified or decides based on exceptions in network communications that the terminal 404 has disconnected.

In association with the login procedure the client 405 may attempt to communicate with the mobile network firewall, gateway or security device 402 it is behind using a firewall configuration interface, such as the Universal Plug and Play (UPnP) Internet gateway configuration protocol (the arrow A in Figure 4). In an alternative embodiment t may do so either before step 601. In either case the client 405 requests the firewall 402 to open an IP hole allowing the server 401 to initiate contact with the client 405 whenever there is need a need thereafter allowing classic prior art mobile application launch as illustrated and described in Figure 3. In the preferred embodiment, the configuration of the firewall 401 to allow incoming messages in this manner is attempted in step 607 immediately after login, and if the security opening operation appears successful (step 608) the server 401 is notified by the client 405. The server 401 then attempts this type of direct IP connection to the client 405 or mobile application 406 (step 609), and if that too is successful (step 610), then one of these test connections is closed and both server 401 and the client 405 mark the second connection as closable (step 611) since they now know that they may save bandwidth charges and resources by closing the connection knowing that server 401 has now gained the ability reopen the connection when

needed for a classic command push procedure (Figure 3, arrow A) or other data communication use. At any time after this point the server 401 or the client 405 may choose to close the remaining network-level connection (usually a TCP or SSL connection) while keeping the application-level "connection" in the form of knowledge of how the server 401 can contact the client 210. The advantage of such an application-level connection without the network-level connection is lower use of network resources particularly on the server side thus significantly increasing server scalability for infrequent command and data push applications by decreasing overhead cost per active user.

Referring to steps 620 and 621 in Figure 6B, after the login and connection setup in Figure 6A, the push client 405 may send a periodic message (the arrow C in Figure 4) from the client 405 to the server 401 to the effect that client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices do not time expire the connection. The period of time (measured in seconds, minutes or hours and varying from mobile network to mobile network) between such periodic messages is set to match the combined needs of all such network devices and network protocols involved in transmitting communication (step 604). The client 405 may then wait for a reply or acknowledgement from the server 401, and if the acknowledgement is received (step 622), the client 405 returns to step 620 to await the next combined connection refresh and test. If the no acknowledgement is received, the client 405 may return to step 604 in Figure 6A to possibly automatically adjust network settings or, if it deems the settings correct but the network not available, simply re-attempt login to the server 401.

Referring to Figure 6C, after the login and connection setup, the push client 405 is ready to receive the push messages over the connection from the server outside the operator's firewall (step 631). If a push message is received, the client 405 executes the corresponding function, such as launch or pass commands and data a mobile application (step 632). If required, the client 405 may also send a message to the server 401 (step 633), such as a command execution acknowledgement or result.

Referring to Figure 6D, after the login and connection setup, the push client 405 may monitor the local resources for a state change (a trigger event) in step 641. If a state change of other event is detected in step 642, the push client 405 may send a message to the server 401 (step 643).

The push server 401 can be server software run on any appropriate computing device. Figures 10A, 10B and 10C are flow diagrams showing examples of processes by which the server 401 maintains a connection with the client 405 and communicates push commands and other data to it.

In step 1001 of Figure 10A, the push server 401 receives a login from the client 405 initiates an attempt to log into the push server 401 over a packet switched network 403, as indicated by the arrow B in Figure 4. In step 1002, a connection is opened to the server 401 and the server 401 is informed of the client's its availability and the details by which the client 405 can be contacted until the server 401 is otherwise notified or detects a network fault or shut-down. In step 1003, the server 401 attempts this type of classic IP push connection to the client 405, and if that is successful (step 1004), then one of these connections is closed and both the server 401 and the client 405 mark the second connection as closable (step 1005).

Referring to steps 1010 and 1011 in Figure 10B, after the login and connection setup, the push server 401 may receive a periodic message (the arrow C in Figure 4) from the client 405 to the effect that the server updates the respective server object associated with a given client so that the connection, server socket or client socket is not time expired as being stale. The server 401 may send a reply or acknowledgement in step 1012 to notify client 405 of successful network, firewall and security traversal.

Referring to step 1021 Figure 10C, after the login and connection setup, the push server 401 monitors for trigger events and event messages. If the server 401 is triggered by a trigger event (the result "yes" in step 1023), it decides based on application-specific logic and/or user preferences whether the resulting push procedure is a BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA procedure in step 1024. In case of BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA, the server 401 sends the command or data push message to the push client 508 through the push client 509 (step 1025). If not using this alternative network connection selected in step 1024, the push server 401 proceeds to step 1026 to perform a more classic COMMAND PUSH or COMMAND PUSH WITH BIDIRECTIONAL DATA. In case of COMMMAND PUSH, the server 401 sends an command push message to the push client 405 and thereby forces a mobile application 406 from a plurality of such push-aware mobile applications in the mobile terminal as specified in the command (step 1026). In the case of COMMAND PUSH WITH

BIDIRECTIONAL DATA, the push server 401 sends the client 405 push commands or data and may return response through the same IP connection (step 1026).

If the server 401 is not triggered by a trigger event (the result "no" in step 1022), it checks whether an event message has been received from the client 405 (step 1023). If not, the process returns to step 1021. If an event message has been received from the client 405, the server checks whether a proximity detection is involved indicating that the mobile terminal 508 can connect to a broadband access point 509 (step 1024). If the broadband access point 509 is connectable, the server 501 performs accordingly, typically by sending an command or data push directly through the broadband access point in a manner described with reference to Figures 5 and 10C (step 1025). If the alternate broadband connection is not available or not preferred in preferences, the server delivers the message directly as above (step 1026).

The above specification, examples and data provide a complete description of the manufacture and use of the system, method, and article of manufacture, i.e., computer program product, of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

Claims

1. A method of pushing commands and data to a wireless terminal from a push server located outside a wireless system serving the wireless terminal, comprising

the push client initiates and maintains over an extended period of time a packet-based data connection through at least one communication security or inter-network connection device of the serving wireless system to the push server using Internet technologies;

the push server sends, in response to predetermined trigger events, at any time push application installation, updates, commands or data messages to be directed to a push application or dynamically loaded module or user interface feature from among a plurality of such applications, modules and features by means of said client-initiated or client-opened and client-maintained permanent connection, whereby avoiding blocking of said server-originated push messages by the security device, and launching said application, application module or dynamically loaded module or user interface feature as needed,

the push client, in response to receiving a push message containing application installation, updates, application commands or data from the push server, forwards such application commands or data or stores such application installation or updates within the mobile terminal to a mobile application from among a plurality of such applications so as to initiate launch optionally to a specified state or if already running initiate or change presentation to the user according to the push message.

2. A method as claimed in claim 1, comprising

the push client sends configuration messages of a security device configuration protocol to the security device to open a path for later server-initiated connection-oriented or connectionless messaging to the push client.

3. A method as claimed in claim 1 or 2, comprising

the security device is a security protocol such as IP6 whereby the client may open the possibility for the server to contact it by exchanging security keys or otherwise enabling subsequent server-initiated contact.

4. A method as claimed in claim 1, 2 or 3, comprising

the push server attempts server-initiated messaging through the security device to the push client after having being informed of the client-initiated connection.

5. A method as claimed in claim 1, 2, 3 or 4, comprising

the push server and the push client after testing the ability of the server to open a connection to the client mark the maintained network-level connection closeable,

the push server and the push client can close said network-level connection while keeping an application level connection information indicating future possibility for the push sever to reopen said network-level connection when needed.

6. A method as claimed in any one of claims 1-5, wherein the step of maintaining further comprises that the push client maintains the permanent connection through the security device by sending periodic keep-alive messages.

7. A method as claimed in any one of claims 1-6, comprising
the push client or the push server sends a periodic reply to messages initiated by the push server or by the push client, respectively, to the effect that the receiving end is informed that the messages are continuing to be received.

the push client or the push server upon failure to receive acknowledgement of said periodic reply may choose to open a new connection.

8. A method as claimed in claim 6 or 7, comprising
use of varying timing between the periodic keep-alive or reply messages to match the combined needs of various network devices involved in transmitting and maintaining communication.

9. A method as claimed in any one of claims 1-8, comprising
if an attempt to contact the push server during initiation of the permanent connection and login is not successful, the push client automatically or under supervision of the user of the wireless terminal tries one or more other techniques, protocols and/or network parameters for contacting the push server.

10. A method as claimed in claim 9, wherein said trying of one or more other techniques and/network parameters include one or more of

using an alternate push server network address which may be more available or more accessible at the present time and from the present location,

using one or more alternative mobile terminal network connection settings, or variation of the parameters within the settings,

using an alternate connection route through a second wireless or fixed terminal accessible to the wireless terminal over a wireless network and capable of communication with the push server,

using a TCP connection,
using a UDP connection,
using an SSL connection,
using an HTTP or tunneling HTTP connection,
using an SHTTP or tunneling HTTPS connection,
using an XML-based connection over other transport protocol.

11. A method as claimed in any one of claims 1-10, comprising the push client stores in the wireless terminal a prioritized data structure listing preferred communication protocols, server addresses, periodic message timings, network access settings, and/or alternate servers and communication routes and uses this data structure to attempt reconnection to the push server if the connection to the server fails.

12. A method as claimed in any one of claims 1-11, wherein the connected networks on which the push server and mobile terminal are located are private networks which allow greater interconnectivity than they both offer to the public Internet.

13. A method as claimed in any one of claims 1-12, wherein the message the push server sends to the push client includes an application launch or reconfiguration push message directing the immediate or subsequent actions and data of the application.

14. A method as claimed in any one of claims 1-13, wherein the push server sends to the push client include an application command or data or reconfiguration message redelivered by the push client as an API call or IP connection between processes running on the same mobile terminal.

15. A method as claimed in any one of claims 1-13, wherein the push server sends to the push client is new application code, application code updates or application data updates.

16. A method as claimed in claim 13-15, wherein the push client is a library or process installed independently or together with but containing or enabling the functionality to supply push messages to one or more of a plurality of applications, modules or dynamically loaded module or user interface features on the mobile terminal.

17. A method as claimed in claim 16 wherein only one of the possible plurality of push clients need operate at a given time, providing push services for a plurality of push-aware applications on the mobile terminal.

18. A method as claimed in any one of claims 1-17, wherein the message the push server sends to the push client includes an optional application launch or event push message triggering the wireless terminal to play a sound notifying the recipient of the message and/or to display notification information such as text, rich text, graphics and rich media from which the user may select or decline to launch the application, dynamically loaded program module or user interface feature based on push message or messages recently received.

19. A method as claimed in 18, wherein the notification sound, text, rich text, graphics and rich media presented by the terminal is selected by and deliverable from the server and may be retrieved from the server by the terminal, thereby allowing the push server to indicate through audio and media signals including note sequences, audio samples sound modification applied to note sequences and audio samples, spoken speech, color, motion, shape and design the message sender, nature, priority, content and other attributes of the received message, message sender and/or message sender current state.

20. A method as claimed in 19, wherein the specified notification information and media is played from a cache in the terminal and the cache is automatically updated over the air as needed with new notification information and media.

21. A method as claimed in any one of claims 1-20, wherein said trigger events include events which the push server is aware of and/or events which the push client is aware of and which a push client from among a plurality of such push clients makes the push server aware of.

22. A method as claimed in any one of claims 1-21, wherein said trigger events include one or more of: the making, receiving, and termination of telephone calls, the transition from presence-to-absence or absence-to-presence of other devices in a physical contact, RF, near field, infrared, personal area, local area, metropolitan area or geographical area wireless communications network, an alarm, notification, videogame action or event, remote application user or application server event, remote user action or inaction, electronic or computing equipment change of state or measurement result.

23. A method as claimed in any one of claims 1-22, comprising the push client in the wireless terminal detects availability of an alternate wireless network connection to a broadband access terminal, or the broadband access terminal detects ability to initiate contact to the wireless terminal,

the push client is responsive to receipt of command and data, application installation and update push messages through said broadband access terminal.

24. A method as claimed in any one of claims 1-23, comprising

the push client in the wireless terminal detects network connection availability of a terminal device with a higher bandwidth capacity or otherwise specified as preferred, or the device with a higher bandwidth capacity detects such ability to connect to the wireless terminal

the push client transmits connection availability information of the higher bandwidth device to the push server, or the large bandwidth terminal transmits connection availability information of the mobile terminal to the push server,

the push server uses the connection availability information as a trigger event for sending lazy or low priority messages including application updates and application data updates routed through the higher bandwidth capacity device to the wireless terminal.

25. A method as claimed in any one of claims 1-24, comprising

the push client in the wireless terminal detects connection availability of a higher bandwidth or more desirable alternate network connection device,

the push client transmits connection availability information of the higher bandwidth device to the push server,

the push server uses the connection availability information as a trigger event for routing messages directed to the user of the wireless terminal through the higher capacity device.

26. A method as claimed in claim 25, comprising

the push server stops directing messages to the higher capacity device when the wireless terminal is no longer connectable to the higher capacity or more desirable alternate wireless network connection device.

27. A method as claimed in any one of claims 24-26, comprising

providing the higher network connectivity device with a push client with server connectivity similar to that in the wireless terminal.

28. A method as claimed in any one of claims 1-27, comprising

the push client in the wireless terminal detects connection availability of a device with a better alternative network connection, or a push client in the device with a better alternative network connection detects connection availability of the wireless terminal,

establishing a data-transfer capability between the push clients,
routing communication to and from the push client in the wireless terminal through the push client and the network connection of the better alternative network connection device.

29. method as claimed in any one of claims 1-28, comprising
customizing the appearance, notification sound or look and feel of the messages received to based on message source, message source state, message parameters or message recipient preferences.

30. A method of pushing messages to a wireless terminal from a push server, comprising

the push server sends, in response to predetermined trigger events, at any time application push messages to a push client in the mobile terminal,

the push client in the wireless terminal detects connection availability of a device with a preferable alternative network connection, or the device with a preferable connection detects connection availability of the wireless terminal,

the push client is responsive to receipt of the application push message to push commands to an application in said device with a larger screen so as to bring forward view an application view identified by, modified by, contained in or otherwise affected in presentation by the received application push message.

31. A method of routing messages to a wireless terminal from a push server, comprising

the push server sends, in response to predetermined trigger events, at any time application push messages to a push client in the mobile terminal,

a push client in the wireless terminal detects a device with a preferred alternative network connection, or a push client in the device with a network connection detects physical proximity of the wireless terminal,

establishing a data-transfer capability between the push clients,

routing communication to and from the push client in the wireless terminal through the push client and the network connection of the device.

32. A method as claimed in any one of claims 1-31 wherein the push client accepts compressed information and optionally decompresses such information for the mobile application.

33. A method as claimed in any one of claims 1-32, wherein the push client and push server establish a secure connection and unwrap such security on behalf of the mobile application.

34. A server comprising means for performing the server steps as claimed in any one of method claims 1-33.

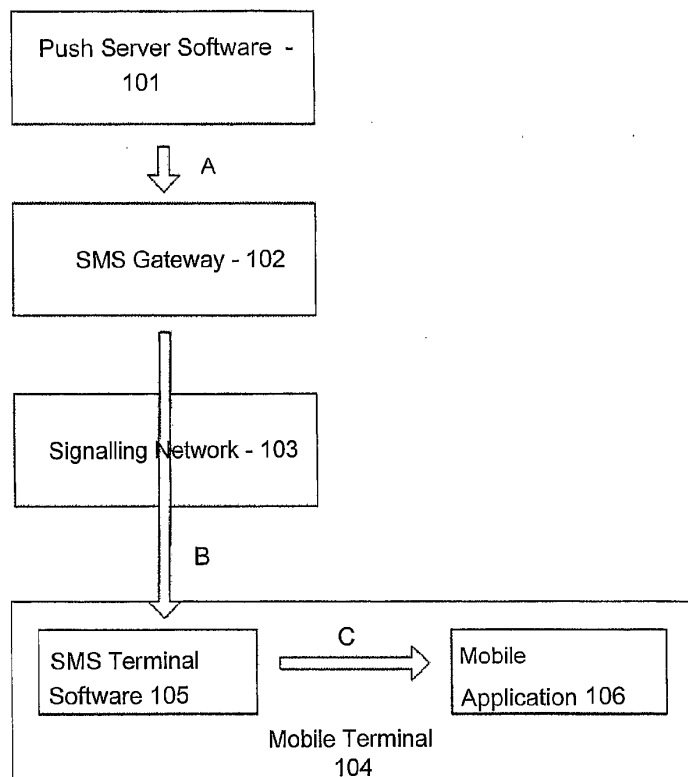
35. A wireless terminal comprising means for performing the push client steps as claimed in any one of method claims 1-34.

36. A program product comprising program code means which, when run in a computing unit of a wireless terminal, performs the push client steps as claimed in any one of method claims 1-35.

37. A program product comprising program code means which, when run in a computing device, performs the push server steps as claimed in any one of method claims 1-37.

1/15

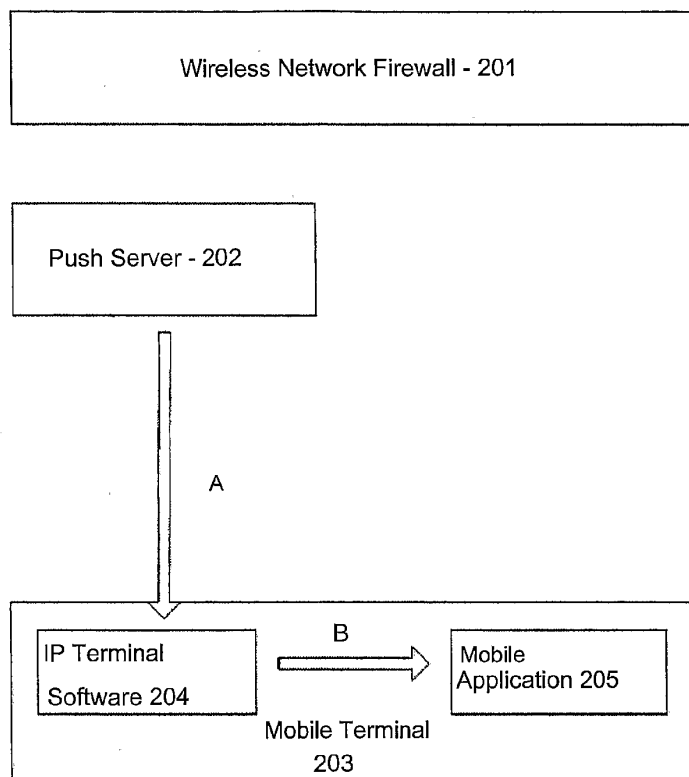
Figure 1



SUBSTITUTE SHEET (RULE 26)

2/15

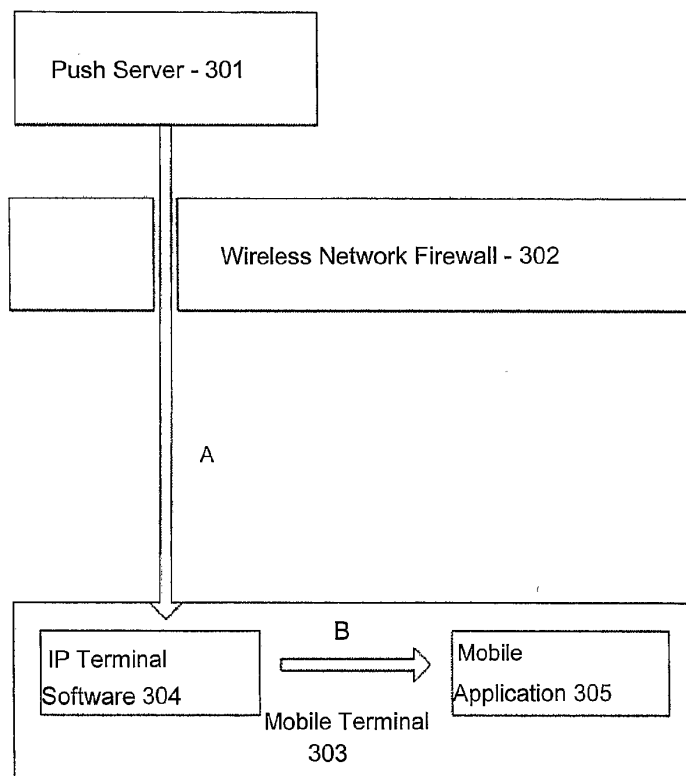
Figure 2



SUBSTITUTE SHEET (RULE 26)

3/15

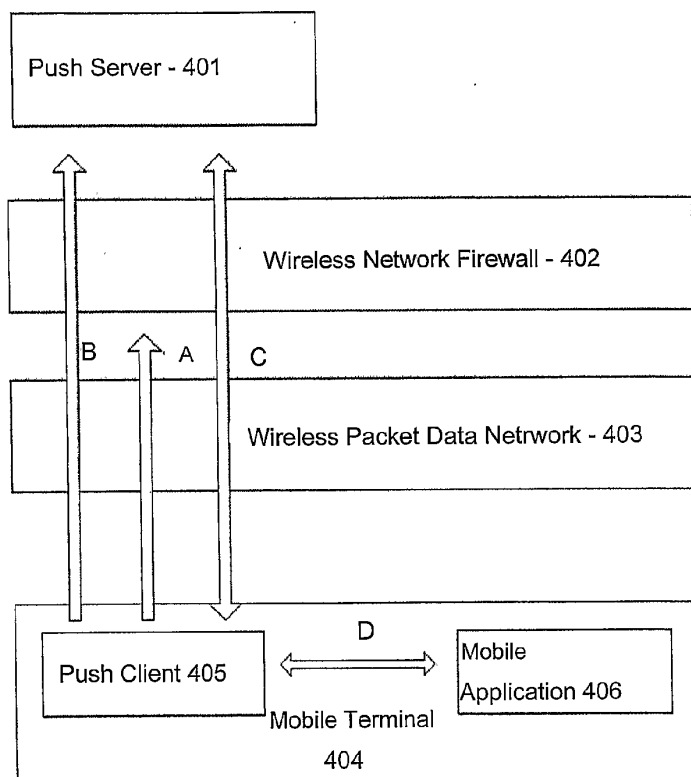
Figure 3



SUBSTITUTE SHEET (RULE 26)

4/15

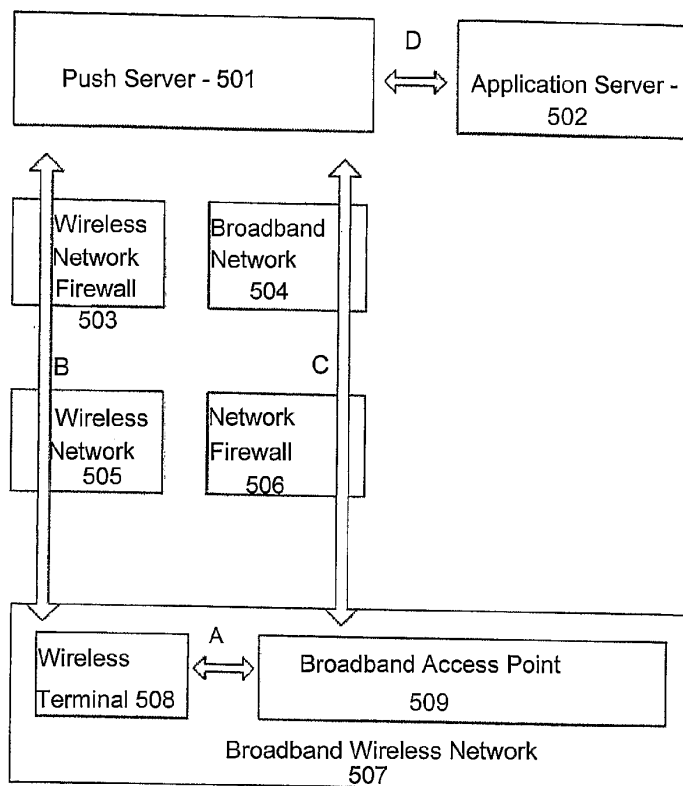
Figure 4



SUBSTITUTE SHEET (RULE 26)

5/15

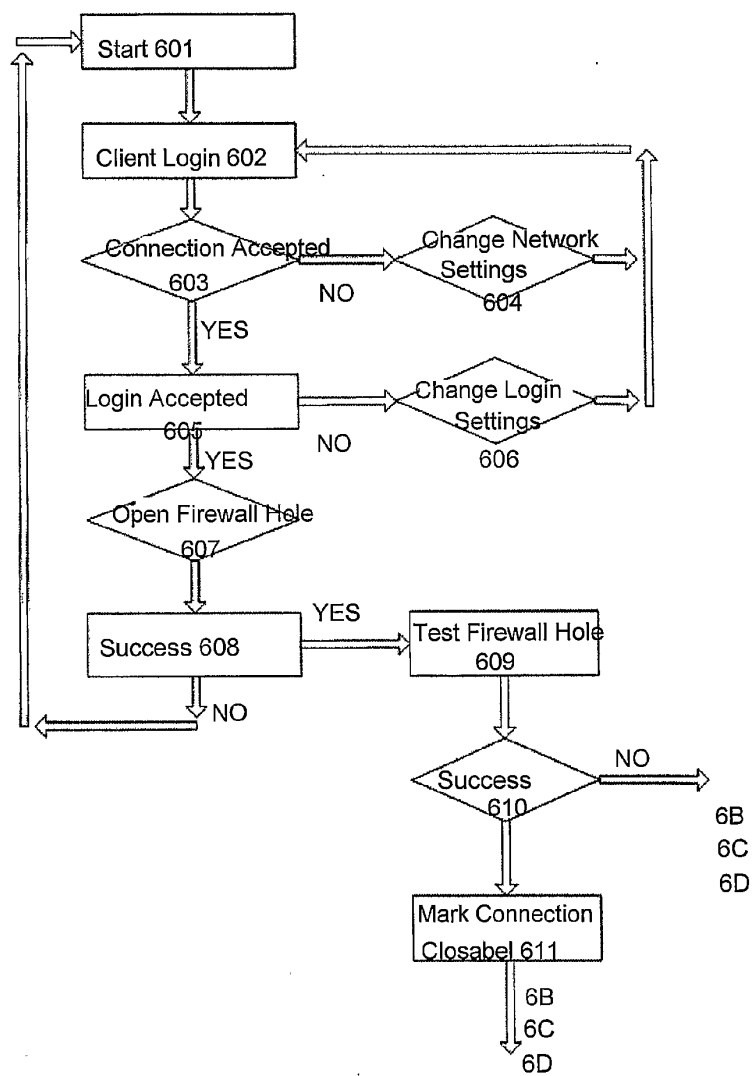
Figure 5



SUBSTITUTE SHEET (RULE 26)

6/15

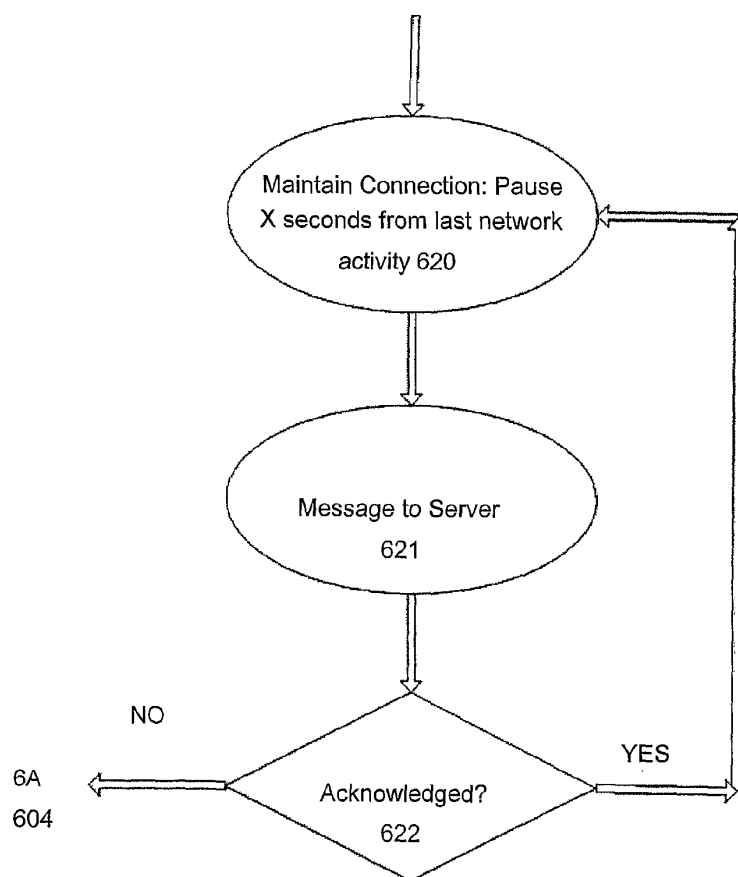
Figure 6A



SUBSTITUTE SHEET (RULE 26)

7/15

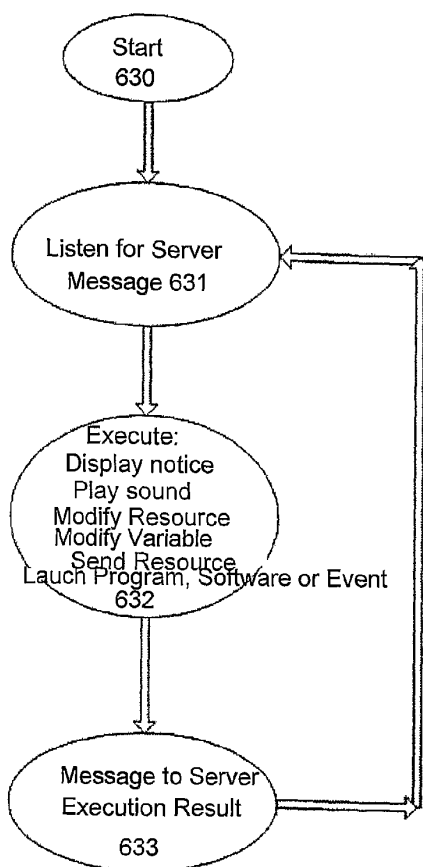
Figure 6B



SUBSTITUTE SHEET (RULE 26)

8/15

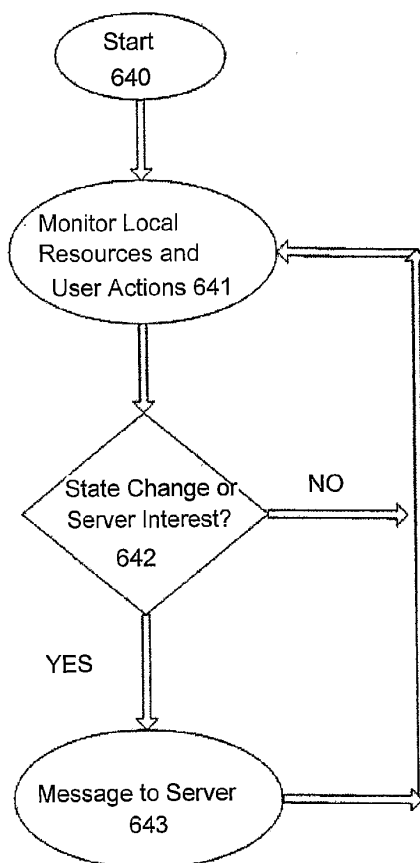
Figure 6C



SUBSTITUTE SHEET (RULE 26)

9/15

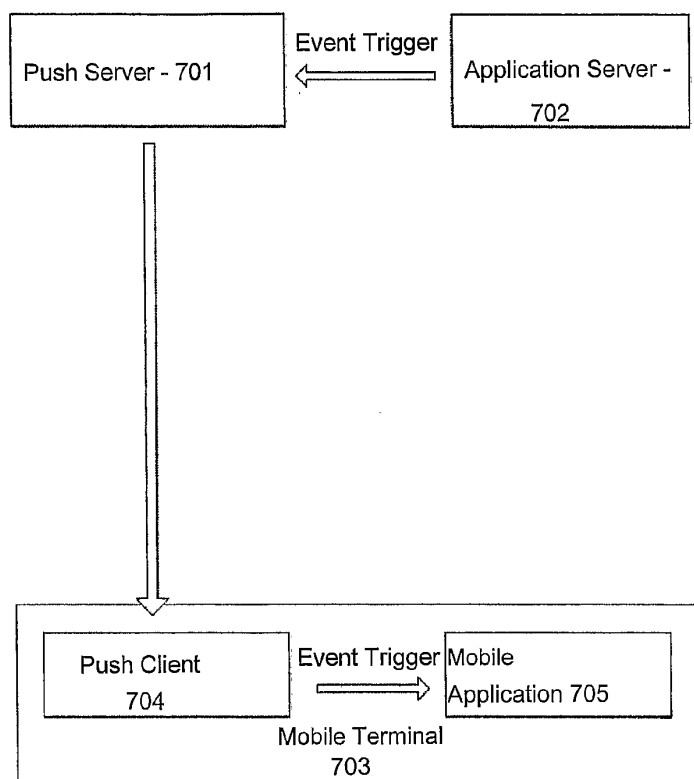
Figure 6D



SUBSTITUTE SHEET (RULE 26)

10/15

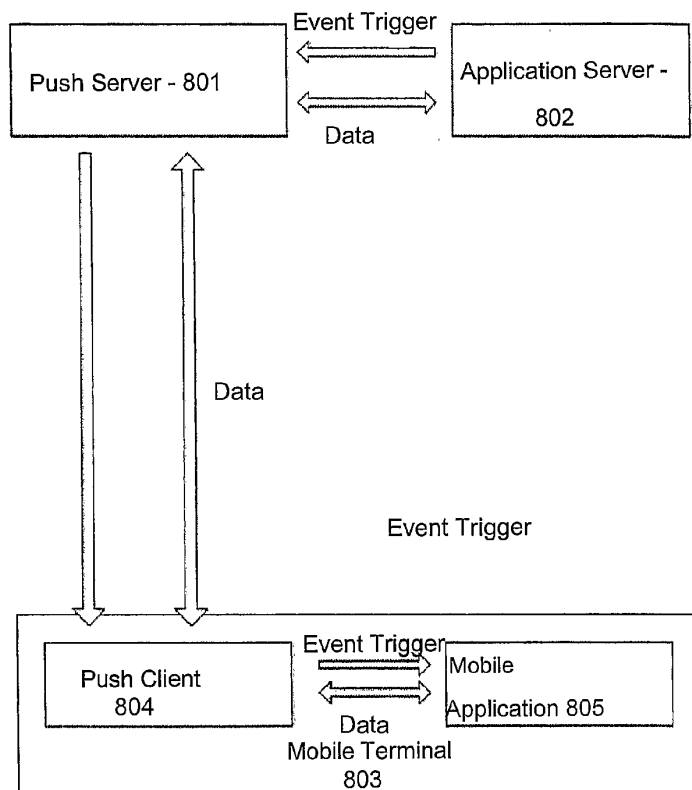
Figure 7



SUBSTITUTE SHEET (RULE 26)

11/15

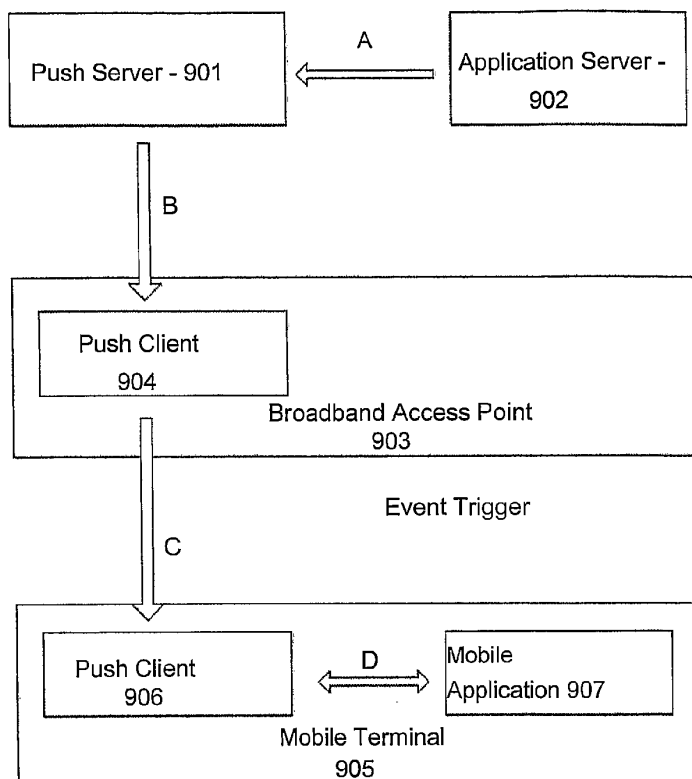
Figure 8



SUBSTITUTE SHEET (RULE 26)

12/15

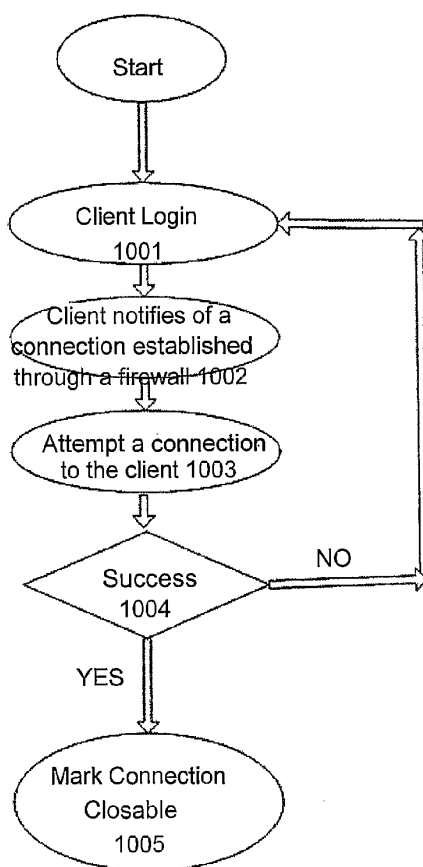
Figure 9



SUBSTITUTE SHEET (RULE 26)

13/15

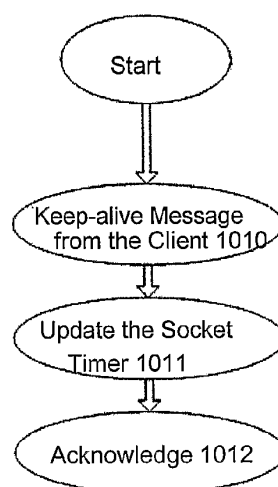
Figure 10A



SUBSTITUTE SHEET (RULE 26)

14/15

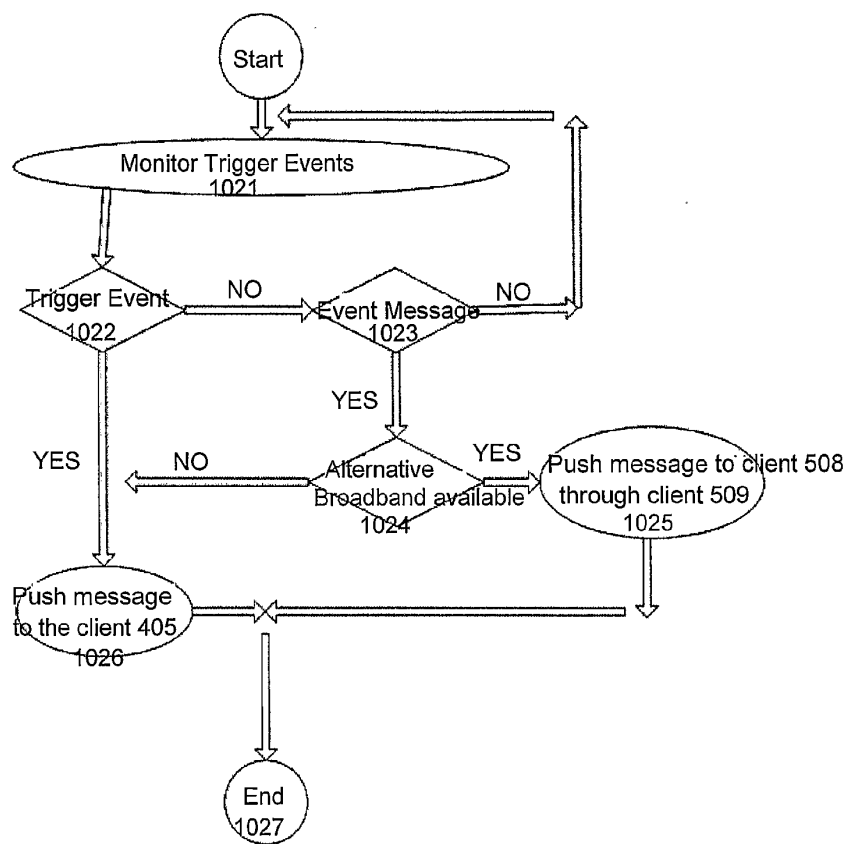
Figure 10B



SUBSTITUTE SHEET (RULE 26)

15/15

Figure 10C



SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2006/050032

A. CLASSIFICATION OF SUBJECT MATTER		
See extra sheet		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC8: H04L, H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
FI, SE, NO, DK		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
EPO-INTERNAL, WPI, PAJ, INSPEC, IEEE Xplore		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2001/0005864 A1 (MOUSSEAU et al.) 28 June 2001 (28.06.2001), Abstract, paragraphs [0003], [0013], [0018], [0071], [0073], [0075]-[0082], fig. 6-9	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
Y	US 2003/0009561 A1 (SOLLEE) 09 January 2003 (09.01.2003), paragraphs [0007], [0027], [0076]	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
Y	WO 02067538 A2 (CELLTICK TECHNOLOGIES LTD et al.) 29 August 2002 (29.08.2002), Abstract, claim 6	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
A	JP 2003134566 A (AICON KK et al.) 09 May 2003 (09.05.2003), Abstract	1-37
A, P	US 2006/0009198 A1 (KASAI et al.) 12 January 2006 (12.01.2006), whole document	1-37
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "Q" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
28 March 2006 (28.03.2006)		10 April 2006 (10.04.2006)
Name and mailing address of the ISA/FI National Board of Patents and Registration of Finland P.O. Box 1160, FI-00101 HELSINKI, Finland Facsimile No. +358 9 6939 5328		Authorized officer Seppo Ojala Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050032

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2001/0005864 A1	28/06/2001	US 2005148356 A1	07/07/2005
		JP 2005100427 A	14/04/2005
		JP 2005100426 A	14/04/2005
		JP 2005056437 A	03/03/2005
		US 2004252727 A1	16/12/2004
		JP 2004220622 A	05/08/2004
		US 2004073619 A1	15/04/2004
		US 2004024824 A1	05/02/2004
		US 2003187938 A1	02/10/2003
		US 2003050987 A1	13/03/2003
		US 2003005066 A1	02/01/2003
		US 2003018816 A1	23/01/2003
		US 2002194285 A1	19/12/2002
		US 2002049818 A1	25/04/2002
		US 2002029258 A1	07/03/2002
		EP 1282957 A2	12/02/2003
		EP 1273136 A2	08/01/2003
		EP 1273135 A2	08/01/2003
		CN 1436413 A	13/08/2003
		WO 0178342 A2	18/10/2001
		WO 0178341 A2	18/10/2001
		WO 0178319 A2	18/10/2001
		CA 2343932 A1	10/10/2001
		CA 2343905 A1	10/10/2001
		CA 2343648 A1	10/10/2001
		AU 5206001 A	23/10/2001
		AU 5020401 A	23/10/2001
		AU 5020101 A	23/10/2001
		US 2001054115 A1	20/12/2001
		US 2002120696 A1	29/08/2002
		US 2001005857 A1	28/06/2001
		US 2001005861 A1	28/06/2001
		US 2001004744 A1	21/06/2001
		US 2001005860 A1	28/06/2001
		US 2001013071 A1	09/08/2001
		US 2001009015 A1	19/07/2001
		MX PA00011592 A	17/10/2002
		NO 20005917 A	26/01/2001
		US 6463463 B1	08/10/2002
		US 6779019 B1	17/08/2004
		US 6463464 B1	08/10/2002
		US 6701378 B1	02/03/2004
		NZ 528050 A	28/01/2005
		NZ 508305 A	30/04/2004
		JP 2002517947T T	18/06/2002
		EP 1082839 A2	14/03/2001
		EP 1320221 A2	18/06/2003
		EP 1315336 A1	28/05/2003

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050032

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
		EP 1206073 A2	15/05/2002
		EP 1126662 A2	22/08/2001
		EP 1124352 A2	16/08/2001
		EP 1098481 A2	09/05/2001
		EP 1096727 A2	02/05/2001
		EP 1096726 A2	02/05/2001
		EP 1096725 A2	02/05/2001
		CN 1304608 A	18/07/2001
		WO 9963709 A2	09/12/1999
		CA 2333881 A1	09/12/1999
		AU 3924499 A	20/12/1999
		AU 758302B B2	20/03/2003
		CA 2511594 A1	29/11/1999
		CA 2367135 A1	29/11/1999
		CA 2356324 A1	29/11/1999
		CA 2356073 A1	29/11/1999
		CA 2356046 A1	29/11/1999
		CA 2356038 A1	29/11/1999
		CA 2356004 A1	29/11/1999
		CA 2245157 A1	29/11/1999
		US 6219694 B1	17/04/2001
.....			
US 2003/0009561 A1	09/01/2003	WO 02103981 A2	27/12/2002
		EP 1446929 A2	18/08/2004
.....			
WO 02067538 A2	29/08/2002	RU 2004116910 A	10/10/2005
		US 2004078427 A1	22/04/2004
		EP 1362491 A2	19/11/2003
		CN 1493165 A	28/04/2004
.....			
JP 2003134566 A	09/05/2003	None	
.....			
US 2006/0009198 A1	12/01/2006	JP 2005108012 A	21/04/2005
.....			

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2006/050032

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.

H04L 12/56 (2006.01)

H04L 29/08 (2006.01)

H04Q 7/22 (2006.01)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
24 April 2008 (24.04.2008)

(10) International Publication Number
WO 2008/048075 A1

(51) International Patent Classification:
H04Q 7/24 (2006.01)

(74) Agent: JIMYUNG Patent Firm, 6F, Jungwoo Bldg.,
1689-1, Seocho-4-dong, Seocho-gu, Seoul 137-882 (KR).

(21) International Application Number:
PCT/KR2007/005155

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG,
ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR,
LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO,
RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TI, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2006-0101714 19 October 2006 (19.10.2006) KR

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,
PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

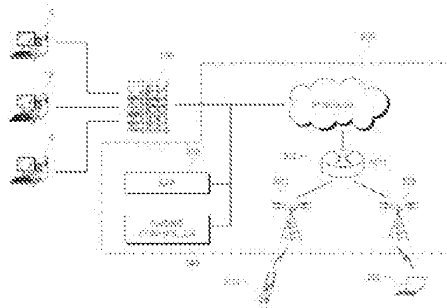
(71) Applicant (for all designated States except US): **INTRO
MOBILE CO., LTD.** [KR/KR]; 2502-Ho, ASEM Tower,
159, Samseong-dong, Gangnam-gu, Seoul 135-798 (KR).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **LEE, Changseok**
[KR/KR]; LG Apt. 101-1602, 12-2, Gaepo-dong, Gang-
nam-gu, Seoul 135-939 (KR).

Published:
— with international search report

(54) Title: SYSTEM OF PROVIDING INTEGRATED PUSH SERVICE AND METHOD THEREOF



(57) Abstract: The present invention relates to a system and a method for providing an integrated push service in an internet service network, and the integrated push service system comprises a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data; an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push; a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information, wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.

WO 2008/048075 A1

Description

SYSTEM OF PROVIDING INTEGRATED PUSH SERVICE AND METHOD THEREOF

Technical Field

- [1] The present invention relates to a system and a method for providing an integrated push service in a network including a mobile internet such as Wibro.

Background Art

- [2] A mobile internet service such as a data service such as WAP (Wireless Application Protocol) based on a mobile communication network such as CDMA2000 1X, 3X, EV-DO, GSM and WCDMA, Wibro (Wireless Broadband) and HPI (High Speed Portable internet) are used to provide a data communication service such as the Internet through a mobile terminal. However, because the mobile communication network is mainly for a voice call and has complex network structure, a cost for building the mobile communication network is high. Therefore, a price per packet is excessive and the mobile communication network is not suitable for the Internet service based on a large capacity multimedia. The mobile internet service is to solve above-described problem wherein a conventional IP network is used to a maximum and a network structure is simple concentrating on a transmission of an IP packet. Therefore, the cost for building the network is low and the price per packet is low. Accordingly, an MBMM (Multiband Multimode) terminal using a conventional CDMA mobile communication modem for the voice call and the mobile internet such as Wibro for a data communication is used.
- [3] On the other hand, a push service is widely used for a sophisticated communication service. The push service actively transmits a data to a client by a server without a user intervention. For instance, an information selected by a user (a news, a stock information and a sports information) is provided to a user terminal in real time or a data for an upgrade is automatically transmitted to the user terminal in order to increase a user convenience.
- [4] However, when the push service is provided via the mobile internet network, problems described below occur.
- [5] First, since a push application server and a push application client should be built for each of the push services, an integrated operation of the network is difficult and a traffic increasing rapidly due to the push service is difficult to manage. In addition, in order to receive the push service in real time, the mobile terminal should load an application or an agent program for each of the push services in a memory. Therefore, a system efficiency is degraded due to a characteristic of the mobile terminal having

limited memory capacity, data processing capacity and battery capacity.

- [6] Second, the mobile terminal enters an idle mode when a data is not transceived considering a mobility of the mobile terminal in case of the mobile internet. In the idle mode, a generation of an unnecessary hand-over traffic is eliminated when moving between base stations in order to minimize a power consumption of the mobile terminal and enable an efficient use of a base station resources. However, in the idle mode, a push data cannot be transmitted to the mobile terminal in real time because the data is not transceived and a connection to a RAS (Radio Access Station) is disengaged.
- [7] Third, since the RAS used in the mobile internet service has a small service coverage compared to a mobile communication base station, a radio frequency shadow area is relatively large and the push data cannot be transmitted in real time when the mobile terminal in the shadow area.

Disclosure of Invention

Technical Problem

- [8] It is an object of the present invention to provide a system and a method for providing an integrated push service wherein various push data generated from a plurality of push application servers are transmitted through an integrated push service server and a mobile terminal extracts an associated application ID app_ID and loads an integrated push service agent selectively invoking a corresponding application to provide the various push services through a mobile internet network, and wherein a separate module for a transmission of the push data is not required for the push service server to reduce a cost for building the push service server, and wherein only a single integrated push service agent is loaded in a memory of the mobile terminal to optimize a system resource of the mobile terminal.
- [9] It is another object of the present invention to provide a system and a method for providing an integrated push service wherein an integrated push service server determines whether a receiving mobile terminal is in an idle mode and a push information is broadcasted via a paging controller provided by a mobile internet service network when the mobile terminal is in the idle mode to provide the push information in real time even to the mobile terminal having a communication session with the integrated push service server terminated in the idle mode.
- [10] It is yet another object of the present invention to provide a system and a method for providing an integrated push service wherein an integrated push service server transmits a push service as an SMS via a mobile communication service network instead of a mobile internet network when a receiving mobile terminal is not connected to the mobile internet network to provide the push information in real time even when

the mobile terminal of a user is in a shadow area of a mobile internet service.

Technical Solution

- [11] In order to achieve above-described object, there is provided an integrated push service system comprising: a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data; an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push; a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information, wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.

- [12] There is also provided a method for providing an integrated push service comprising steps of: (a) transmitting a push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data and an associated application ID specifying the application for invoking the push data to an integrated push service server through a communication network; (b) transmitting the push information to the receiving mobile terminal via an IP push through a mobile internet service network using the integrated push service server; and (c) receiving the push information using an integrated push service agent resident in a memory of the mobile terminal, and invoking the application compliant to the associated application ID to deliver the push data.

Advantageous Effects

- [13] In accordance with the system and the method for providing the integrated push service of the present invention, the various push data generated from the plurality of push application servers are transmitted through the integrated push service server and the mobile terminal extracts the associated application ID app_ID and loads the

integrated push service agent selectively invoking the corresponding application to provide the various push services through the mobile internet network, the separate module for the transmission of the push data is not required for the push service server to reduce the cost for building the push service server, and only the single integrated push service agent is loaded in the memory of the mobile terminal to optimize the system resource of the mobile terminal.

[14] In accordance with the system and the method for providing the integrated push service of the present invention, the integrated push service server determines whether the receiving mobile terminal is in the idle mode and the push information is broadcasted via the paging controller provided by the mobile internet service network when the mobile terminal is in the idle mode to provide the push information in real time even to the mobile terminal having the communication session with the integrated push service server terminated in the idle mode.

[15] In accordance with the system and the method for providing the integrated push service wherein the integrated push service server transmits the push service as the SMS via the mobile communication service network instead of the mobile internet network when the receiving mobile terminal is not connected to the mobile internet network to provide the push information in real time even when the mobile terminal of the user is in the shadow area of the mobile internet service.

Brief Description of the Drawings

[16] Fig. 1 is a diagram illustrating a configuration of an integrated push service system in accordance with an embodiment of the present invention.

[17] Fig. 2 is a diagram illustrating a configuration of an integrated push service server in accordance with an embodiment of the present invention.

[18] Fig. 3 is a diagram illustrating a configuration of an integrated push service agent in accordance with an embodiment of the present invention.

[19] Fig. 4 is a diagram illustrating a hierarchy of an integrated push service agent in accordance with an embodiment of the present invention.

[20] Fig. 5 is a diagram illustrating a configuration of an integrated push service agent in accordance with an embodiment of the present invention.

[21] Figs. 6 through 8 are diagrams illustrating a communication system of a method for providing an integrated push service in accordance with an embodiment of the present invention.

Mode for the Invention

[22] Fig. 1 is a diagram illustrating a configuration of an integrated push service system in accordance with an embodiment of the present invention. Referring to Fig. 1, the integrated push service system comprises a plurality of push application servers 10, 12

and 14, an integrated push service server 100, a mobile internet service network 300, and a mobile terminal 200 including an integrated push service agent 250. The plurality of push application servers 10, 12 and 14 provides a push data to a push service application stored in the mobile terminal 200. The plurality of push application servers 10, 12 and 14 generate the push data push_data such as a real time news data for a news application, a chatting message for a peer-to-peer messenger application and an e-mail message for an e-mail application. A push information push_info including a receiving mobile terminal information specifying the mobile terminal that receives the push data, and an associated application ID app_ID specifying the application for invoking the push data along with the push data is also generated.

- [23] In accordance with a conventional push application server, the associated application ID app_ID is not required because the conventional push application server is built for a single push application and a communication session and a protocol are maintained for each of the servers. However, in accordance with the present invention, various push services provided to each of applications are managed in an integrated fashion through the integrated push service server 100 and the integrated push service agent 250. Therefore, the associated application ID app_ID specifying the application for invoking the push data is required.
- [24] <Transmission of the push information through an IP push>
- [25] The integrated push service server 100 receives the push information push_info from the plurality of push application servers 10, 12 and 14 connected through a communication network, and provides the push information push_info to the mobile terminal 200 through an IP push push_IP. Because the mobile terminal 200 maintains a communication session with the integrated push service server 100 through a CSM (Communication Session Manager) 251 of the integrated push service agent 250, the push information push_info including the push data may be transmitted through the IP push push_IP. When the push information push_info is transmitted through the IP push push_IP, the integrated push service server 100 requests the IP push to the mobile internet service network 300.
- [26] The mobile terminal 200 transmits a push information acknowledge message ack_push to the integrated push service server 100 when the push information push_info is received. the integrated push service server 100 acknowledges a successful transmission of the push data by receiving the push information acknowledge message ack_push at a reception acknowledge unit 142. A transmission report manager 140 transmits an information on the reception and a push application service to each of the plurality of push application servers 10, 12 and 14 as a transmission report.
- [27] The mobile internet service network 300 is a high speed wireless internet service

such as Wibro and HPI which carries out a communication between the integrated push service server 100 and the mobile terminal 200, transmission/reception of the IP push data push_IP.

[28] The mobile terminal 200 receives the push information push_info in a form of the IP push push_IP through a mobile internet modem 210 for connecting to the mobile internet service network 300, and includes at least one application 260 that is to be associated with the push information push_info. Particularly, the mobile terminal 200 includes the integrated push service agent 250. The integrated push service agent 250 includes the CSM 251 resident on a memory of the mobile terminal 200 that maintains the communication session with the integrated push service server 100 in a state that the mobile internet modem 210 is connected to the mobile internet service network 300, and selectively invokes the application 260 compliant to the associated application ID app_ID of the push information push_info to deliver the push data.

[29] When an entirety of the applications 260 supporting a plurality of push services such as a chatting service, a mail service, a news service and a stock service in the mobile terminal 200 are resident in the memory in order to correspond to individual IP push in accordance with conventional art, a system resources of the mobile terminal 200 may be overloaded to degrade a processing speed thereof and is wasted. However, as shown in Fig. 3, only the integrated push service agent 250 of the mobile terminal 200 is resident in the memory of the mobile terminal 200 with each of the applications 260 being inactive in accordance with the embodiment of the present invention while an IP push receiver 252 receives the push information push_info for the entirety of the applications in an integrated fashion and uses the associated application ID app_ID included in the push information push_info to selectively invoke the application 260 corresponding to the associated application ID app_ID, thereby reducing a number of the applications resident in the memory and a power consumption of the mobile terminal 200.

[30] <Transmission of push information via paging message>

[31] On the other hand, a mobile internet service generally supports a power saving mode in order to reduce power consumption in a mobile environment. The mobile terminal 200 typically updates to which RAS 320 of a plurality of RASs 320 and 322 through a constant communication and a hand-over with the RASs 320 and 322. However, an unnecessary power consumption occurs for the mobile terminal 200 that does not have a constant transmission/reception of a data in order to maintain the constant communication with the mobile internet service network 300 for the hand-over and a registration of the RAS. As a result, the unnecessary power consumption has a serious effect on a DBDM(dual-band dual-mode) terminal using both the mobile internet service network 300 and a mobile communication service network 400 such as

a CDMA and a GSM or MBMM(multi-band multi-mode) terminal supporting three or more communication services.

- [32] The power saving mode provided by the mobile internet service is to solve above-described problem. In the power saving mode, the mobile terminal 200 enters an idle mode wherein a connection to the RAS 320 is lost when an exchange of the data with a mobile internet network is not carried out for more than a predetermined time. The idle mode refers to a state that the transmission/reception of the data by the mobile terminal 200 is not carried out and the connection to the RAS 320 is lost to eliminate a generation of an unnecessary hand-over traffic between the mobile terminal 200 and the RASs 320 and 322, thereby minimizing the power consumption of the mobile terminal 200 and enabling an efficient use of the RASs 320 and 322.
- [33] When a packet to be transmitted to the mobile terminal 200 is generated in the idle mode, a paging controller 340 of the mobile internet service network 300 broadcasts a paging message through the RASs 320 and 322 of a paging group consisting of the plurality of RASs wherein the mobile terminal 200 expected to exist. Through this process, the mobile terminal 200 receives a downlink data packet to exit the idle mode and enter a normal mode to re-connect to the mobile internet service network 300.
- [34] In accordance with the embodiment of the present invention, a push service may be provided continuously for the mobile terminal 200 in the idle mode by transmitting the push information through the paging message. When the mobile terminal 200 enters the idle mode, the CSM 251 of the integrated push service agent 250 of the mobile terminal 200 cannot send the push information push_info through the IP push push_IP because the communication session with the integrated push service server 100 is terminated. While the integrated push service server 100 may schedule and transmit the push information push_info or re-transmit the push information push_info by recognizing a communication configuration of the mobile terminal 200, the push service cannot be provided in real time.
- [35] It is preferable that the push information push_info is included in the paging message instead of the IP push push_IP such that the push service is provided to the mobile terminal 200 in real time in order to solve above-described problem.
- [36] There are two methods for the mobile terminal 200 to recognize the idle mode of the mobile terminal 200. In accordance with a first method, whether the mobile terminal 200 is in the idle mode is registered in a presence server 130 such that the integrated push service server 100 may inquire the presence server 130 of whether the mobile terminal 200 is in the idle mode prior to transmitting the push information push_info. In accordance with a second method, the integrated push service server 100 transmits the push information push_info by the IP push push_IP and determines that the mobile terminal 200 is in the idle mode when the push information acknowledge

message ack_push is not received from the mobile terminal 200.

- [37] While a configuration of the integrated push service server 100 is complex due to an association with the presence server 130, an unnecessary IP push is omitted to enable an efficient use of a network resource in accordance with the first method. While an unnecessary traffic is generated due to the IP push push_IP, the integrated push service server 100 does not require the association with the presence server 130, thereby simplifying a system configuration in accordance with the second method.

- [38] The first method wherein the presence server 130 is used is described below in detail.

- [39] In accordance with first method, the integrated push service server 100 or the mobile internet service network 300 further includes the presence server 130 that determines whether the mobile terminal 200 is in the idle mode, and also further comprises the paging controller 340 for broadcasting the paging message for the mobile terminal 200 through the at least one RASs 320 and 322. The integrated push service server 100 provides the push information push_info to the paging controller 340 when the mobile terminal 200 is determined to be in the idle mode using the presence server 130, and the integrated push service agent further comprises a paging message parser 253 for parsing the push information push_info when the push information push_info is received as the paging message push_paging.

- [40] In accordance with first method, the integrated push service server 100 inquires the presence server 130 of whether the mobile terminal 200 is in the idle mode and transmits the push information push_info as the paging message push_paging through the paging controller 340 instead of the IP push push_IP in the idle mode. The mobile terminal 200 extracts the push data push_data and the associated application ID app_ID from the paging message push_paging through the paging message parser 253 as the paging message push_paging is received. The corresponding application 260 is then invoked to provide various push services between the plurality of push application servers 10, 12 and 14 and the mobile terminal 200.

- [41] The second method wherein the presence server 130 is not used is described below in detail.

- [42] In accordance with second method, the integrated push service agent 250 further comprises a reception acknowledge report manager 256 for generating the push information acknowledge message ack_push, and the mobile internet service network 300 further comprises the paging controller 340 for broadcasting the paging message for the mobile terminal 200 through the at least one RASs 320 and 322. The integrated push service server 100 provides the push information push_info to the paging controller 340 when the push information acknowledge message ack_push is not received from the reception acknowledge report manager 256, and the mobile terminal

200 is configured to further include the paging message parser 253 for parsing for parsing the push information push_info when the push information push_info is received as the paging message push_paging.

[43] In accordance with second method, the integrated push service server 100 transmits the push information push_info via the IP push push_IP and determines that the mobile terminal 200 is in the idle mode when the push information acknowledge message ack_push is not received. The mobile terminal 200 extracts the push data push_data and the associated application ID app_ID from the paging message push_paging through the paging message parser 253 as the paging message push_paging is received. The corresponding application 260 is then invoked to provide various push services between the plurality of push application servers 10, 12 and 14 and the mobile terminal 200.

[44] In accordance with the embodiment wherein the push information push_info is transmitted through the paging message push_paging, it preferable that the CSM 251 of the integrated push service agent 250 of the mobile terminal 200 controls the mobile internet modem 210 to configure the communication session between the integrated push service server 100 and the integrated push service agent 250. In case that the push data push_data is too large to be transmitted efficiently by only the paging message push_paging or that other data is to be transmitted after the transmission of the push information push_info, the mobile terminal 200 automatically exits the idle mode to configure the communication session with the integrated push service server 100 when the push information push_info is received as the paging message push_paging, thereby efficiently providing the push service.

[45] <Transmission of push information through SMS of service network>

[46] Since the mobile internet service is designed for a data communication, the mobile internet service is disadvantageous over the mobile communication service such as CDMA and GSM. Considering the disadvantage, a DBDM terminal or a MBMM terminal supporting both the mobile communication service and the mobile internet service is used. In such case, the mobile terminal 200 includes the mobile internet modem 210 and a mobile communication modem 220.

[47] However, in accordance with embodiment, while the mobile internet modem 210 maintains the communication with the mobile communication service network 400 in order to receive an incoming call, a communication with the mobile internet service network 300 for the data communication is established selectively when required by a user. In addition, since the mobile internet service network 300 has a small service coverage compared to the mobile communication service network 400, the communication with the mobile communication service network 400 is frequently terminated when the mobile terminal 200 enters a shadow area.

- [48] When the mobile terminal 200 is unable to establish the communication with the mobile communication service network 400, the push data push_data cannot be transmitted via the IP push push_IP or the paging message push_paging even when a new push data push_data is generated in a push application server 10.
- [49] In such case, the integrated push service agent 250 connects to the paging controller 340 and informs the integrated push service server 100 of the mobile terminal 200 entering the network once connected to the mobile internet service network 300. the integrated push service server 100 searches whether the push information push_info that is not transmitted to the mobile terminal 200 exists to transmit the push information push_info as the IP push push_IP or the paging message push_paging. However, the push service is not provided in real time even in accordance with the embodiment.
- [50] In order to solve above-described problem, the integrated push service system further comprises the mobile communication service network 400 including a plurality of base stations and a SMSC, the mobile terminal 200 further comprises the mobile communication modem 220 for connecting to the mobile communication service network 400, the integrated push service server 100 transmits the push information push_info to the SMSC of the mobile communication service network 400 when the mobile terminal 200 is determined to be disconnected from the mobile internet service network, and the integrated push service agent 250 further comprises an SMS parser 254 for parsing the push information push_info when the push information push_info is received via an SMS push_SMS through the mobile communication modem 250.
- [51] In accordance with the embodiment, a real time push service is possible since the push information push_info may be transmitted via the SMS push_SMS even when the mobile terminal 200 is not connected to the mobile internet service network 300.
- [52] On the other hand, in a certain case, the push data push_data should be transmitted to the application 260 using a data service provided by the mobile communication service network 400 such as WAP (wireless Application Protocol) instead of the application 260 using the mobile internet service network 300. Typically, a method wherein a connection to a data network of a corresponding mobile communication service via the SMS is used. In such case, the integrated push service agent 250 may be configured to further include a mobile communication service interface. The integrated push service agent 250 further comprises the mobile communication service interface for controlling the mobile communication modem 220 to connect to the data network provided by the mobile communication service network 400, and may be configured to control the mobile communication modem 220 to connect to the data network of the mobile communication service network when the associated application ID app_ID of the received push information push_info designates the application 260 associated with

the data network of the mobile communication service network 400.

- [53] <Method for providing integrated push service>
- [54] Figs. 6 through 8 are diagrams illustrating a communication system of a method for providing an integrated push service in accordance with an embodiment of the present invention.
- [55] First steps (S100 and S120) are carried out wherein a push information push_info including a push data push_data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data push_data and an associated application ID app_ID specifying the application for invoking the push data push_data is transmitted to an integrated push service server through a communication network.
- [56] Thereafter, second steps S200 and S210 are carried out wherein a integrated push service server 100 transmits the push information push_info to the receiving mobile terminal 200 via an IP push through a mobile internet service network 300.
- [57] Thereafter, third steps S500 and S600 are carried out wherein an integrated push service agent 250 resident in a memory of the mobile terminal 200 receives the push information push_info (S500) and invokes an application 260 compliant to the associated application ID app_ID to deliver the push data push_data.
- [58] The embodiment is described in detail wherein the push information push_info is transmitted as a paging message push_message in order to provide the integrated push service even when the mobile terminal 200 is in an idle mode.
- [59] First, the method for providing the integrated push service further comprises a fourth step wherein a presence server 130 detects the idle mode of the mobile terminal 200 prior to the first steps S100 and S120, the second steps S200 and S210 further comprises a first sub-step S305 wherein the push information push_info is requested to a paging controller 340 of the mobile internet service network 300 to be transmitted as the paging message push_paging when the mobile terminal 200 is determined to be in the idle mode, and a second sub-step S310 wherein the paging controller 340 broadcasts the push information push_info as the paging message push_paging through at least one RASs 320 and 211, and the third step S600 may be configured in a manner that the integrated push service agent 250 parses the paging message push_paging to extract the push information push_info.
- [60] In accordance with the embodiment shown in Fig. 7 wherein the presence server 130 is not used, the third step further comprises a third sub-step (S700) wherein the integrated push service agent 250 transmits a reception acknowledge message ack_push to the integrated push service server according to the reception of the push information push_info, the second steps S200 and S210 further comprises a first sub-step S305 of requesting a paging controller of the mobile internet service network to

transmit the push information push_info as the paging message push_paging when the reception acknowledge message is not received and a fifth sub-step S310 wherein the paging controller 340 broadcasts the push information push_info as the paging message push_paging through at least one RASs 320 and 322, and the third step S600 may be configured to in a manner that the integrated push service agent 250 parses the paging message push_paging to extract the push information push_info.

[61] After carrying out the third step S600, the integrated push service agent 250 may further establish a communication session with the integrated push service server according to the reception of the push information push_info.

[62] Finally, an embodiment of the method for providing the integrated push service using the SMS wherein the mobile terminal 200 is a DBDM terminal that may connect to the mobile internet service network 300 and the mobile communication service network 400 and the mobile terminal 200 is not connected to the mobile internet service network 300 to provide the integrated push service in real time is described below in detail.

[63] As shown in Fig. 8, the second steps S200 and S210 comprises a sixth sub-step wherein the push information push_info is transmitted to an SMSC of the mobile communication service network 400 when the mobile terminal 200 is determined to be disconnected from the mobile internet service network 300 and a seventh sub-step wherein the SMSC transmits the push information push_info to the receiving mobile terminal 200 as the SMS push_SMS, and the third steps S500 and S600 further comprises an eighth sub-step wherein the integrated push service agent 250 parses the received SMS push_SMS to extract the push information push_info.

[64] While the present invention has been particularly shown and described with reference to the preferred embodiment thereof, it will be understood by those skilled in the art that various changes in form and details may be effected therein without departing from the spirit and scope of the invention as defined by the appended claims.

Claims

- [1] An integrated push service system comprising:
 a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data;
 an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push;
 a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and
 the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information,
 wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.
- [2] The system in accordance with claim 1, wherein the integrated push service server or the mobile internet service network further comprises a presence server for detecting an idle mode of the mobile terminal,
 wherein the mobile internet service network further comprises a paging controller for broadcasting a paging message for the mobile terminal through the at least one RAS,
 wherein the integrated push service server provides the push information to the paging controller when the mobile terminal is determined to be in the idle mode through the presence server, and
 wherein the integrated push service agent further comprises a paging message parser for parsing the push information when the push information is received as the paging message.
- [3] The system in accordance with claim 1, wherein the integrated push service

agent further comprises a reception acknowledge report manager for generating a push information reception acknowledge message according to the reception of the push information.

wherein the mobile internet service network further comprises a paging controller for broadcasting a paging message for the mobile terminal through the at least one RAS,

wherein the integrated push service server provides the push information to the paging controller when the push information reception acknowledge message is not received from the reception acknowledge report manager after transmitting the push message via an IP push, and

wherein the mobile terminal further comprises a paging message parser for parsing the push information when the push information is received as the paging message.

[4] The system in accordance with one of claims 2 and 3, wherein the communication session manager establishes a communication session between the integrated push service server and the integrated push service agent by controlling the mobile internet modem when the push information is received as the paging message.

[5] The system in accordance with one of claims 2 and 3, wherein the integrated push service server stores the push information when the mobile terminal is not connected to the mobile internet service network and transmits the stored push information when the mobile terminal is connected to the mobile internet service network.

[6] The system in accordance with claim 5, wherein the integrated push service agent informs the integrated push service server of an entrance to the mobile internet service network via the paging message by connecting to the paging controller when connected to the mobile internet service network.

[7] The system in accordance with one of claims 1 through 3, further comprising a mobile communication service network including a plurality of base stations and a SMSC,

wherein the mobile terminal further comprises a mobile communication modem for connecting to the mobile communication service network,

wherein the integrated push service server transmits the push information to the SMSC of the mobile communication service network when the mobile terminal is determined to be disconnected from the mobile internet service network, and

wherein the integrated push service agent further comprises an SMS parser for parsing the push information when the push information is received via an SMS through the mobile communication modem.

- [8] The system in accordance with claim 7, wherein the integrated push service agent the integrated push service agent further comprises a mobile communication service interface for controlling the mobile communication modem to connect to a data network provided by the mobile communication service network, and controls the mobile communication modem to connect to the data network of the mobile communication service network when the associated application ID of the received push information designates the application associated with the data network of the mobile communication service network.
- [9] The system in accordance with one of claims 1 through 3, wherein the integrated push service server further comprises a transmission report manager for generating a transmission report including a result of a push information transmission, and transmits the result of the push information transmission to the push application server providing the push information.
- [10] A method for providing an integrated push service comprising steps of:
 (a) transmitting a push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data and an associated application ID specifying the application for invoking the push data to an integrated push service server through a communication network;
 (b) transmitting the push information to the receiving mobile terminal via an IP push through a mobile internet service network using the integrated push service server; and
 (c) receiving the push information using an integrated push service agent resident in a memory of the mobile terminal, and invoking the application compliant to the associated application ID to deliver the push data.
- [11] The method in accordance with claim 10, further comprising (d) detecting an idle mode of the mobile terminal by a presence server prior to the step (a), wherein the step (b) further comprises:
 (a-1) requesting the push information as a paging message using a paging controller of the mobile internet service network when the mobile terminal is determined to be in the idle mode; and
 (a-2) broadcasting the push information as the paging message through at least one RAS using the paging controller, and
 wherein the step (c) comprises extracting the push information by parsing the paging message using the integrated push service agent.
- [12] The method in accordance with claim 10, wherein the step (c) further comprises (c-1) transmitting a reception acknowledge message to the integrated push service server according to the reception of the push information using the

integrated push service agent,

wherein the step (b) further comprises:

(b-1) requesting a paging controller of the mobile internet service network to transmit the push information as the paging message when the reception acknowledge message is not received; and

(b-2) broadcasting the push information as the paging message through at least one RAS using the paging controller, and

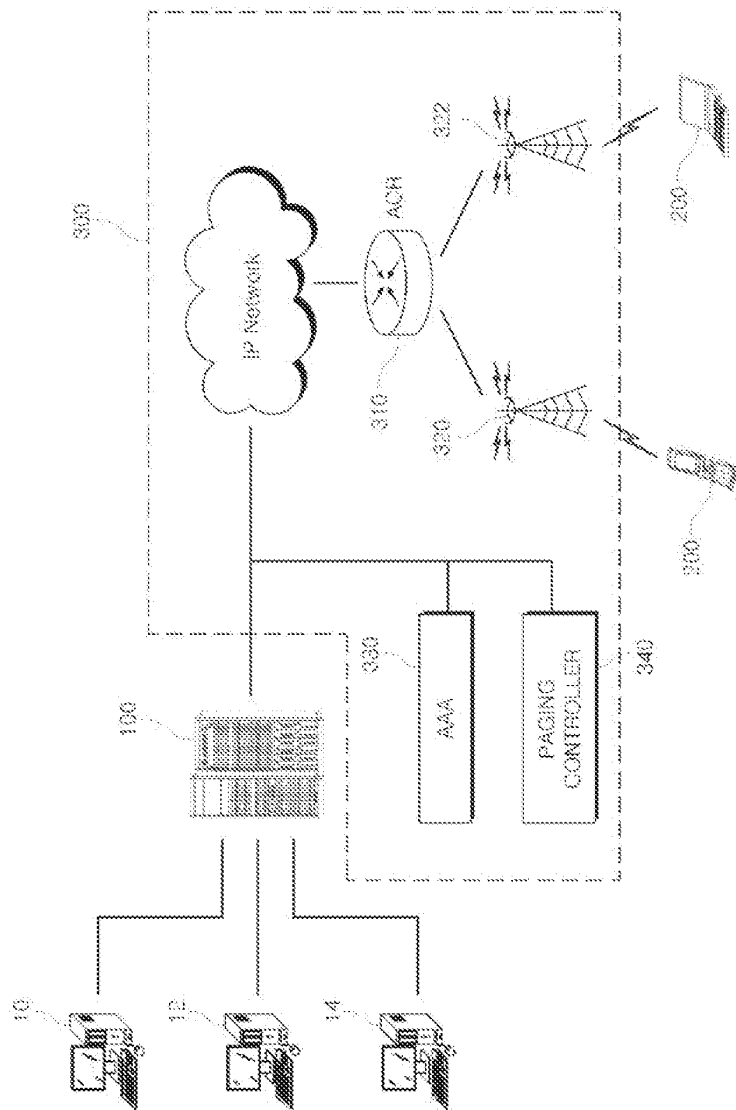
wherein the step (c) extracting the push information by parsing the paging message using the integrated push service agent.

[13] The method in accordance with one of claims 11 and 12, wherein further comprising (e) establishing a communication session between the integrated push service server and the integrated push service agent according to the reception of the push information after carrying out the step (c).

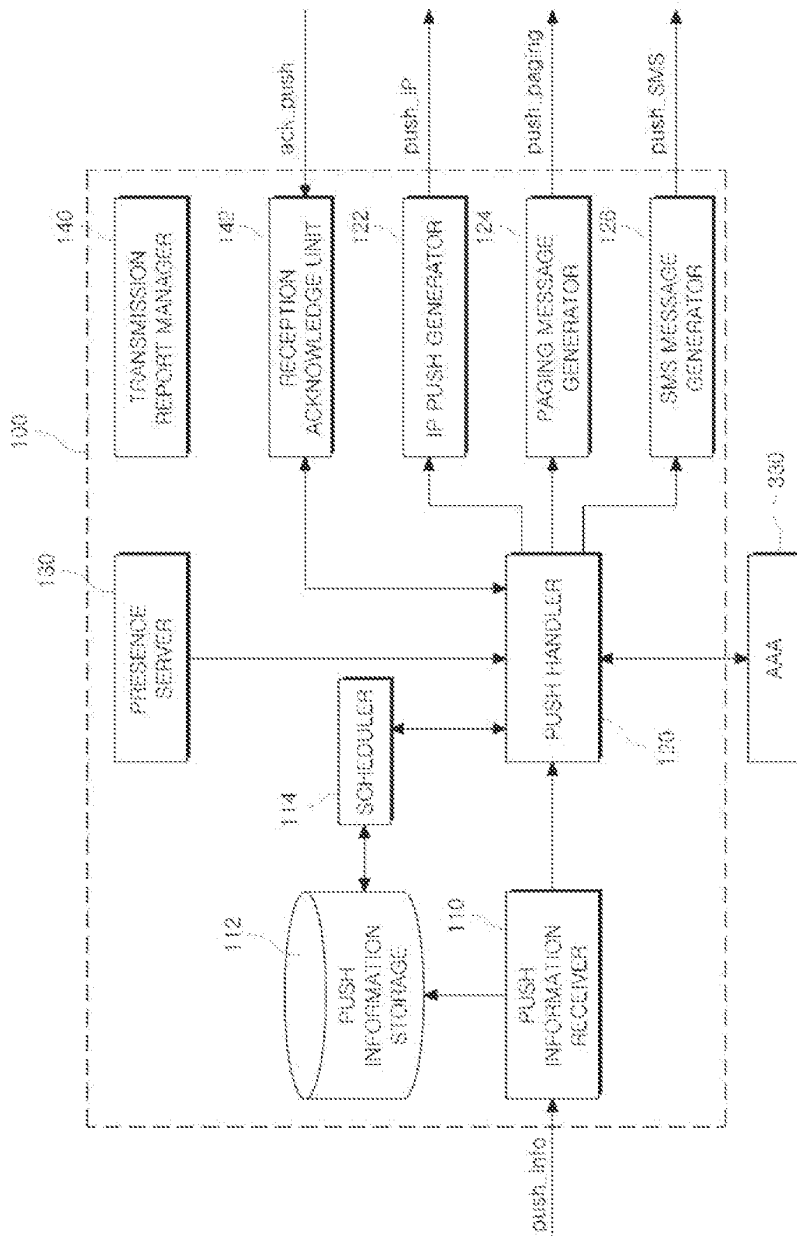
[14] The method in accordance with one of claims 11 and 12, wherein the step (b) comprises storing the push information when the mobile terminal is not connected to the mobile internet service network, and re-transmitting the stored push information when the mobile terminal is connected to the mobile internet service network.

[15] The method in accordance with one of claims 11 and 12, wherein the step (b) comprises:
(b-3) transmitting the push information to a SMSC of the mobile internet service network when the mobile terminal is determined to be disconnected from the mobile internet service network; and
(b-4) transmitting the push information to the receiving mobile terminal as an SMS by the SMCC, and
wherein the step (c) further comprises (c-2) extracting the push information by parsing the SMS by the integrated push service agent.

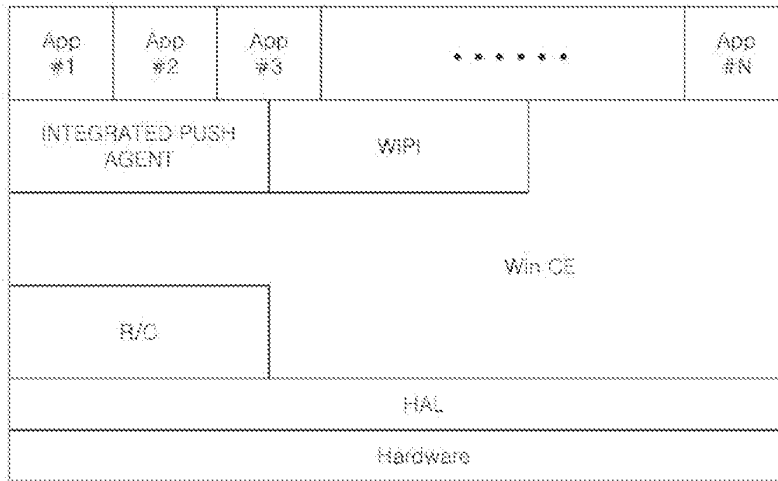
[Fig. 1]



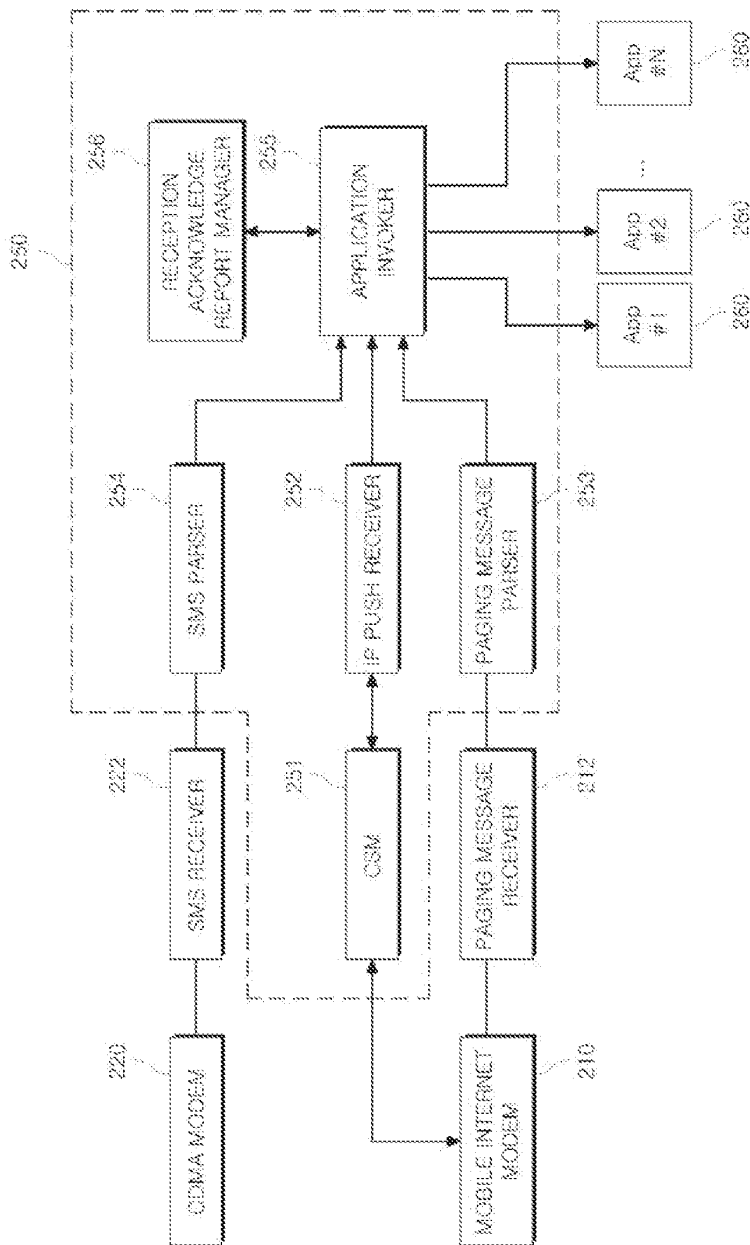
[Fig. 2]



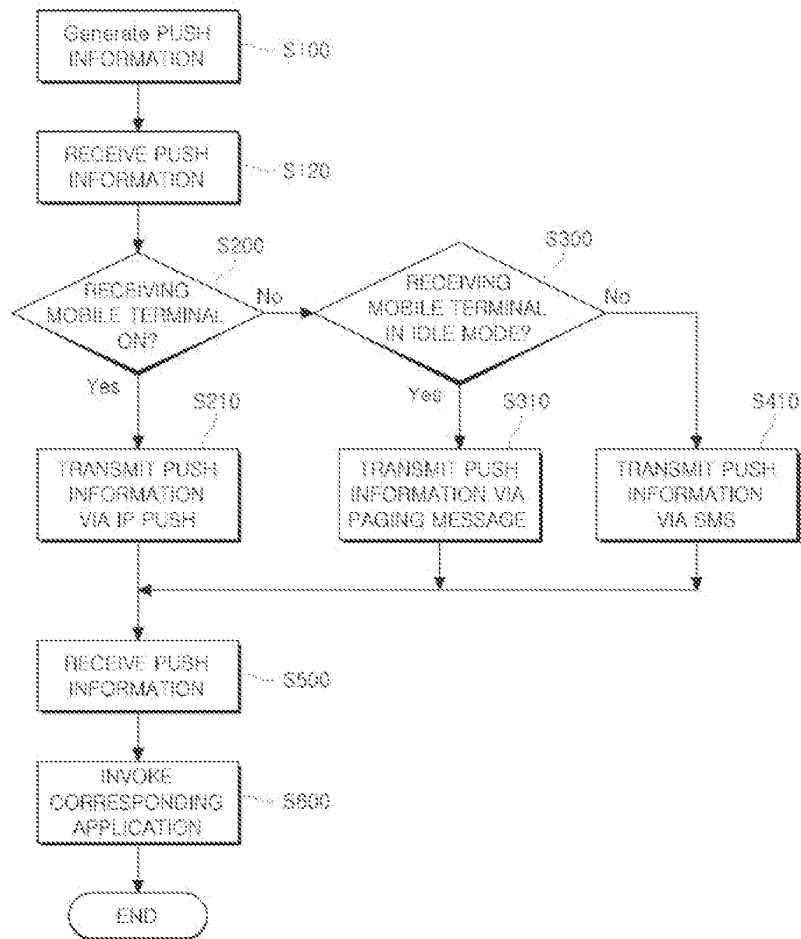
[Fig. 3]



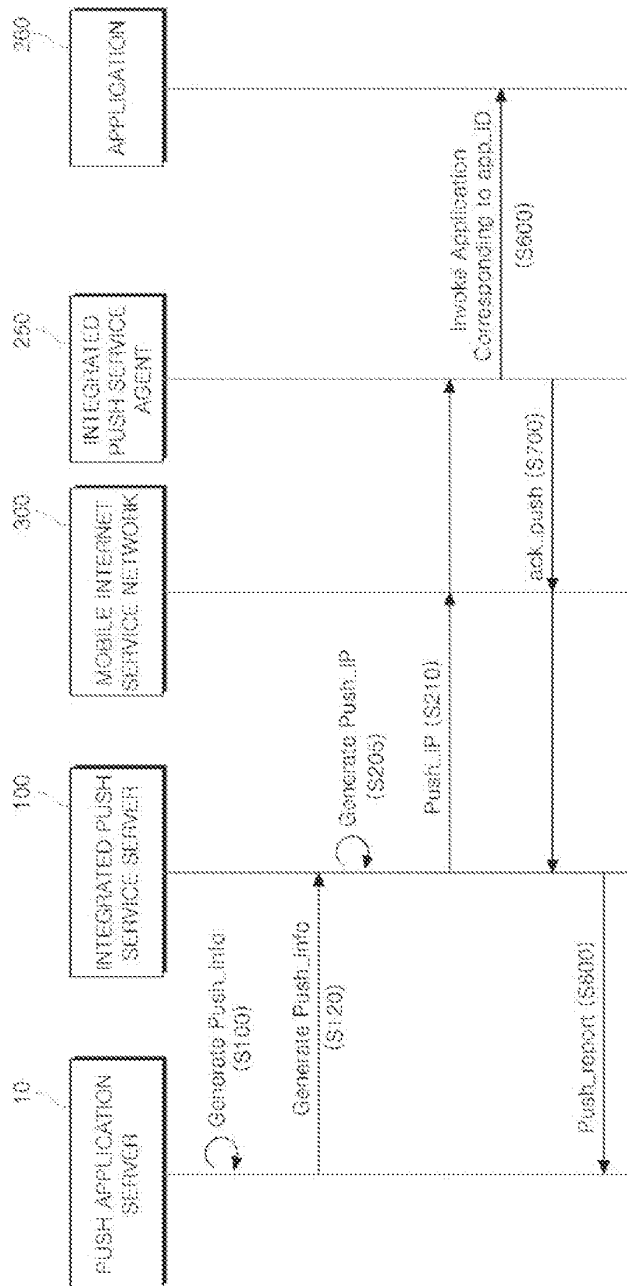
[Fig. 4]



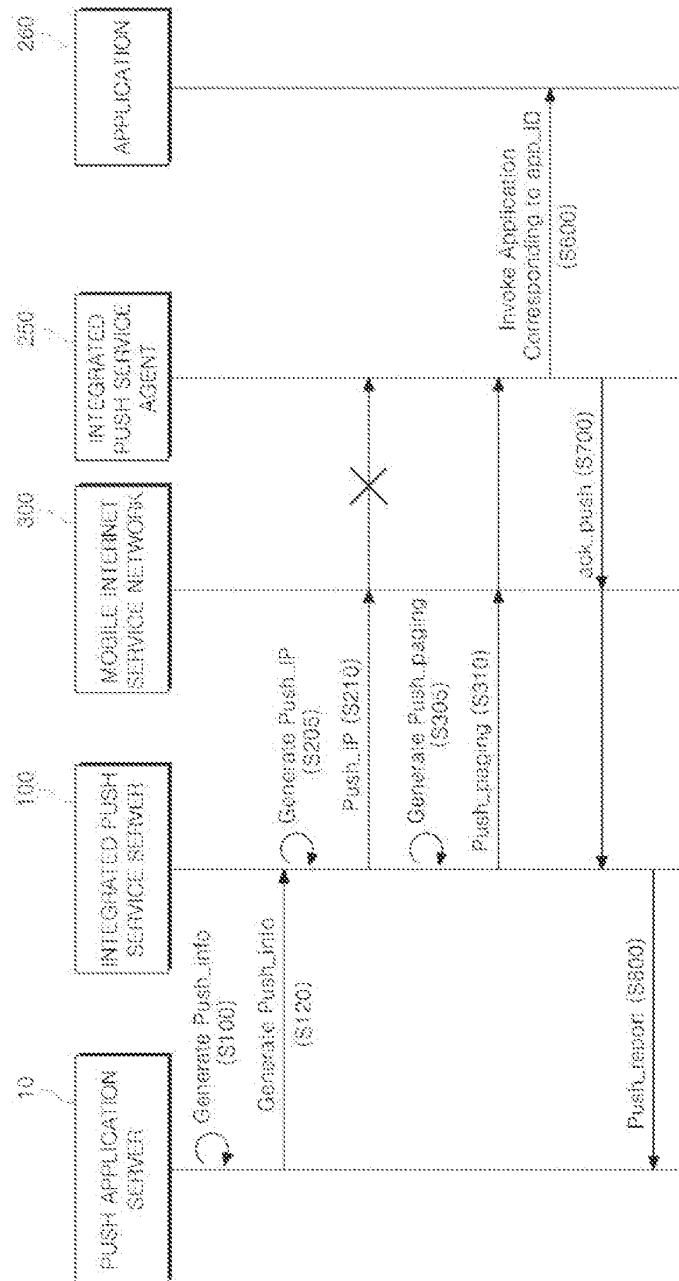
[Fig. 5]



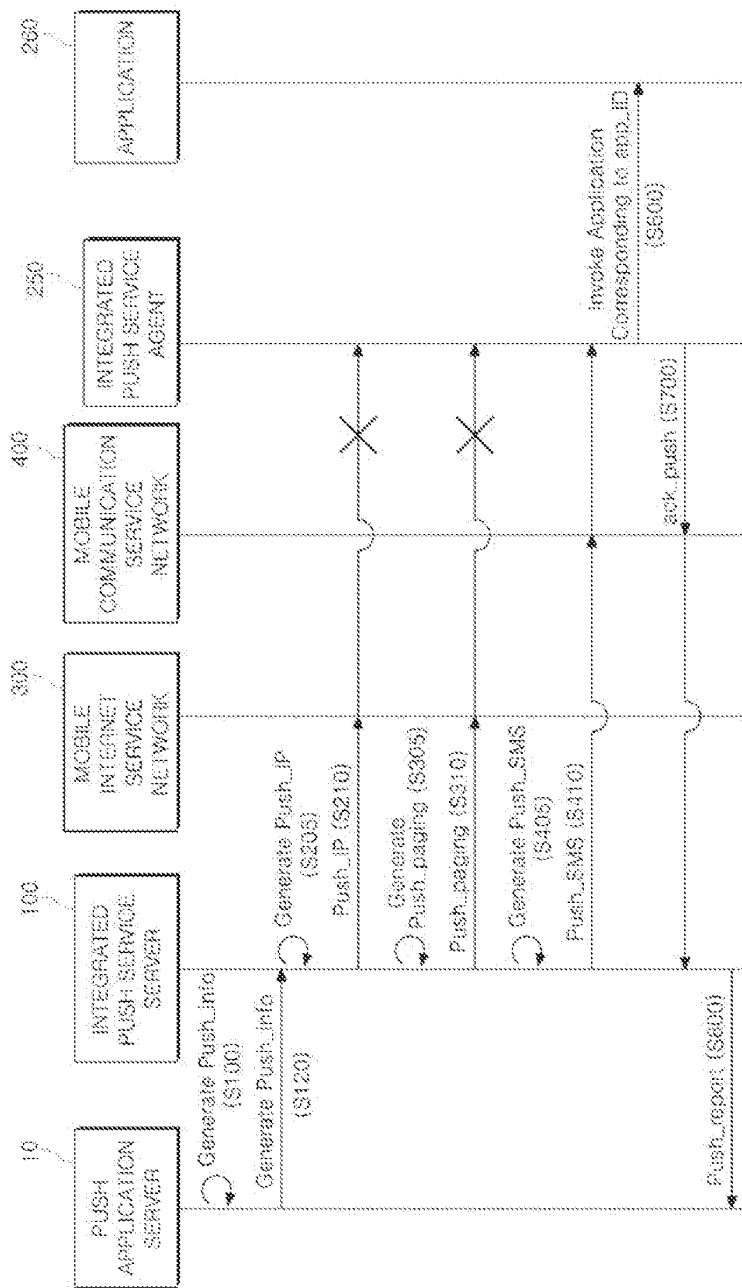
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/005155**A. CLASSIFICATION OF SUBJECT MATTER***H04Q 7/24(2006.01)I*

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : H04Q 7:24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility Models since 1975

Japanese Utility models and applications for Utility Models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS(KIPO internal) "push, application, server, agent"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 06999991 B1 (Ikeda, H.) 14 Feb. 2006 See abstract, figures 1-2, claims 1-9, and column 6, line 53 - column 8, line 5	1-15
A	US 2002-0116472 A1 (Kalish, D. et al.) 22 Aug. 2002 See abstract, figures 1-2, claims 1-10, and paragraphs [0020]-[0032]	1-15
A	KR 10-2003-0037448 A (SK TELECOM CO., LTD.) 14 May 2003 See abstract, figure 2, claims 1-5, and page 3, lines 20-47	1-15
A	EP 10-2004-0045803 A (WIDERTHAN.COM CO., LTD.) 02 Jun. 2004 See abstract, figures 3-4, claims 1-4, and page 4, line 57 - page 6, line 9	1-15
A	KR 10-2005-0064905 A (LG ELECTRONICS INC.) 29 Jun. 2005 See abstract, figure 3, claims 1-3, and page 3, lines 1-15	1-15
A	EP 10-2001-0008959 A (SK TELECOM CO., LTD.) 05 Feb. 2001 See abstract, figures 1-2, claims 1-6, and page 3, line 11 - page 4, line 4	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

26 DECEMBER 2007 (26.12.2007)

Date of mailing of the international search report

27 DECEMBER 2007 (27.12.2007)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Kwang Sik

Telephone No. 82-42-481-8355



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/005155

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 06999991 B1	14.02.2006	None	
US 20020116472 A1	22.08.2002	WO2003068064A1	23.10.2003
KR 1020030037448 A	14.05.2003	None	
KR 1020040045803 A	02.06.2004	None	
KR 1020050064905 A	29.06.2005	None	
KR 1020010008959 A	05.02.2001	None	



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION # 17/577,237	RECEIPT DATE / TIME 01/24/2024 08:30:52 PM Z ET	ATTORNEY DOCKET # RALEP007C11C3C2C3C2C1C1C1
------------------------------------	---	---

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	64077226	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 20

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1C1C1_IDS_1_24_24.pdf	7	Information Disclosure Statement (IDS) Form (SB08)	1254 KB
EP1909463A1.pdf	64	Foreign Reference	8013 KB
WO2006077283A1.pdf	56	Foreign Reference	7072 KB
WO2008048075A1.pdf	27	Foreign Reference	4559 KB
Exhibit 1035 RDF Primer.pdf	62	Non Patent Literature	4762 KB
Exhibit 1036 Yahoo RSS Reader.pdf	1	Non Patent Literature	670 KB
Exhibit 1037 Nokia E71 Review.pdf	8	Non Patent Literature	1334 KB
Exhibit 1014 Dierks The	76	Non Patent Literature	6294 KB

Transport Layer Security TLS
Protocol V. 1.1.pdf

Exhibit 1018 European Telecommunications Standards Institute.pdf	21	Non Patent Literature	6206 KB
Exhibit 1013 FreierThe SSL Protocol v3.0.pdf	17	Non Patent Literature	967 KB
Exhibit 1004 3GPP TS- 23.140_Part1-1.pdf	99	Non Patent Literature	24407 KB
Exhibit 1004 3GPP TS- 23.140_Part2-1.pdf	119	Non Patent Literature	22393 KB
Exhibit 1029 Dictionary of Computer Scitence.pdf	3	Non Patent Literature	3382 KB
Exhibit 1028 Mostafa.pdf	12	Non Patent Literature	851 KB
Exhibit 1011 Open Mobile Alliance OMA-ERELD-MMS- v1_2.pdf	16	Non Patent Literature	850 KB
Exhibit 1012 Open Mobile Alliance Multimedia Messaging Service Architecture Overview- MMSARCH.pdf	26	Non Patent Literature	7983 KB
IPR2024-00341 Petition.pdf	94	Non Patent Literature	1066 KB
IPR2024-00342 Petition.pdf	97	Non Patent Literature	2447 KB
Exhibit 1021-Plaintiff Disclosure of Asserted Claims and Infringement Contention.pdf	88	Non Patent Literature	9003 KB
Exhibit 1038 HW Amended Infringe Contentions.pdf	108	Non Patent Literature	7009 KB

Digest

DOCUMENT

RALEP007C11C3C2C3C2C1C
1C1_IDS_1_24_24.pdf

EP1909463A1.pdf

MESSAGE DIGEST(SHA-512)

F91D7B451BDF7CCCD968CEAF56B26D5854B91744612EB6F7
9C076DAE173F466FC60BCB9C43716E012B340E316B387AE6D
C9B33600392E96F575103AD03EDC3D7

6D85A90D83B8FCF4E64CC822F2575148043B4905F370992F98

	87496C2A4F77754B5747DD3C13C5CCCF2EDB7CEAA3F247C C9EF97C7900958B48162E6EE7306FEB
WO2006077283A1.pdf	FC572CDA9102D1FB70FA4477514E9114E12B9DF5F6626B114 CF7E52F5310A7ADF467167B85A3BAC5519A58838492B8029D 71893C95C2AD8006BAE14FF525F938
WO2008048075A1.pdf	6E9631DA73DF1F24E4582C2C53265ED16E2C23896DEFADAA F8B07E266706C784AD5CBCA17AE1C3966F5FF03B4F5382187 F34FDA44CEBBBC73CC299E893F86369
Exhibit 1035 RDF Primer.pdf	8E8B964C9B0580969D67484CA42794A53ACDE6BF1CB3DD69 86FB48A255635F07E687511D82B058F9C9798F97356AACDCC 91629B9B589F1F1425A7798D88028B9
Exhibit 1036 Yahoo RSS Reader.pdf	B972BDEF69775250AF10476CF6089ACEAEC8E7BF9C082B46 3032378134EE4016D5A376F51044CBB9DAF6BF582FE8778F65 D2138063640A2B1A7455F400A7359B
Exhibit 1037 Nokia E71 Review.pdf	8F29E6B53F03EE1955CA0DA21AA7E8D7F0DDD9A9312C93FF 94FFBE84F7067242A24C3187697B8ECDFA80E8F4E00FD6337 294A568418D663C3A9A154DED1F4040
Exhibit 1014 Dierks The Transport Layer Security TLS Protocol V. 1.1.pdf	6775ED61A9417ED622CA810F15BDBD4ACEE13B90C7785E21 42E946EF4CE10E20164E01ABF67597A6538B77D25248F71112 C6269F7772BF522CB788B943FCFB58
Exhibit 1018 European Telecommunications Standards Institute.pdf	598643CB2F2D6987944E949EFF1EDB7F29AEE3D1AD9545C5 A30628FD6ABD9F9D0B128B31B6276834B99029D83A53893955 89AC06B35AB4DF43F1F63495E8AA59
Exhibit 1013 FreierThe SSL Protocol v3.0.pdf	EA900AC9DE8528B11E029CA69D6BBF80E12D506816CF6B84 E72F560DF670B6C40F3B284B85FDED51D60E8393A4BFE6714 5797397A4B384181DFF766FBF8C9576
Exhibit 1004 3GPP TS- 23.140_Part1-1.pdf	3B90E0F06DEE659CA340AA816CB24376E81C0016D218B9B34 C796BE10C5B03FBC45A0DB5AB082737A100E957F082C2F72 D17C3CD27B59F21790942472CE5DD46
Exhibit 1004 3GPP TS- 23.140_Part2-1.pdf	BDC8CADA0E4F21565FC5FEC10675ABBB6E54EFA7E665A00 E68C4D9696B0EAE6C2AA5A5449ACB63FFE9026DE90625616 8C5FF1AA9E6F16B91A0ACA4EBF73148E7
Exhibit 1029 Dictionary of Computer Scitence.pdf	3043364D1DEFA6829F644033B0DFD1A1B0763CA86EAAC5DA 9517B37EE951CFEF88A2376E2FAE55718F25079D34B64D8FD CAA6D2988B1E9050E9AD72F2BE72E11
Exhibit 1028 Mostafa.pdf	572F1EED03A1821B6BE3F373519102FC54FF9F1223F33E0344 2700B94F63D7A8E501BD4C406E7DD6032C23CABB1431F1D4 219AFFD3223E0EA5126160A182BDB7
Exhibit 1011 Open Mobile Alliance OMA-ERELD-MMS- v1_2.pdf	9497DD367A83A6524657C3FA835A981E09F432C4F56B90C64 B74F9657FE291049B8F611D95534713BF83FBB2AD694A54B1 A2C10AAA8298E9BBB111F898EEE7C6

Exhibit 1012 Open Mobile Alliance Multimedia Messaging Service Architecture Overview-MMSARCH.pdf	4DAA75D61ED58C0D18579E2EEEF80EC6442D78BA4EE1D957969425037884D7738FE6750920A77267909FD437520063403B51B33A37A07EC7E245A780DC048BE5
IPR2024-00341 Petition.pdf	6ED1DA14D90EA9C0E9AEAD27FF03D6BC76251E5A16690456E1C1E57006CCC8D8C118598B1E156A0778EC9F5A18AFF3EB2BDD1AFDBC8D1BD5A644217BCDED9B14
IPR2024-00342 Petition.pdf	410E0459EAF8FFFC7A36940F46ECB28619543EBFEB390F29C6D6B6414D12B5A3A7CAA798AA6EFE7FF7D1D84C518E8D444F4F6E68B187BE2FB94F161FF7EAF75
Exhibit 1021-Plaintiff Disclosure of Asserted Claims and Infringement Contention.pdf	C38189D9628B2130D3B0147104BD9612F04EC1818DFE49B108329A0B144FC27682B1321A89FC17B9089DC7C63B78AA919A95437FBD1CBFAEEA1295F3F0E9409A
Exhibit 1038 HW Amended Infringe Contentions.pdf	D7D6BAD76AAA059C3C66632A392162D36493866EC6324E60211597CB550C44ADC87FE7705E555C32E0E905EAA4F43EC6863A5C4959C1AEB2BAC7EF53DC60C9B7

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	6101485	A	2000-08-08	Fortenberry et al.		
	2	7509487	B2	2009-03-24	Lu et al.		
	3	7844915	B2	2010-11-30	Platzer et al.		
	4	7975147	B1	2011-07-05	Qumei		
	5	8010669	B2	2011-08-30	Sathish		
	6	8195961	B2	2012-06-05	Ogawa		
	7	8370818	B2	2013-02-05	Osminer et al.		
	8	8406733	B2	2013-03-26	Raleigh		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit			
	Examiner Name			
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C	

	9	9032192	B2	2015-05-12	Frank	
	10	8620988		2013-12-31	Sohm	
	11	5581704		1996-12-03	Barbara	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030096625	A1	2003-05-22	Lee et al.	
	2	20050207379	B2	2011-04-12	Shen et al.	
	3	20090037270	A1	2009-02-05	Patro	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1909463	EP	B1	2016-09-21	Hwang et al.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit			
	Examiner Name			
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C		

	2	2006077283	WO	A1	2006-07-27	Houghton et al.		☐
	3	2008048075	WO	A1	2008-04-24	Lee		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	"RDF Primer" W3C Recommendation 10 February 2004	☐
	2	Baker, Loren, "Yahoo's RSS Reader goes LIVE on My Yahoo" January 26, 2004	☐
	3	Cha, Bonnie, "Nokia E71 review: Nokia E71" July 2, 2008	☐
	4	Dierks, T., "The Transport Layer Security (TLS) Protocol Version 1.1", April 2006	☐
	5	ETSI TC AT-Features, "Work on MMS for PSTN/ISDN in AT-F" March 12, 2003	☐
	6	Freier, Alan, et al, "The SSL Protocol Version 3.0", March 1996	☐
	7	Global System for Mobile Communications; 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Function description; Stage 2 (Release 6) March 2005	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C

	8	Laplane, Phillip, "Dictionary of Computer Science, Engineering and Technology"; ISBN 0-8496-2691-5	☐
	9	Miaj-E-Mostafa, "Transporting data between wireless applications using a messaging system -- MMS" July 7, 2006	☐
	10	Open Mobile Alliance; "Enabler Release Definition for MMS Version 1.2" September 23, 2003	☐
	11	Open Mobile Alliance; "Multimedia Messaging Service Architecture Overview Version 1.2" September 20, 2003	☐
	12	IPR2024-00341: Petition for Inter Partes Review of United States Patent No. 8,406,733, filed on January 23, 2024	☐
	13	IPR2024-00342: Petition for Inter Partes Review of United States Patent No. 8,406,733, filed on January 23, 2024	☐
	14	File History of IPR2024-00341; filed on January 23, 2024	☐
	15	File History of IPR2024-00342; filed on January 23, 2024	☐
	16	Plaintiff Headwater Research LLC's Disclosure of Asserted Claims And Infringement Contentions, Headwater Research LLC v. Samsung Electronics Co., 6:23-cv-00103-JRG-RSP (WDTX)	☐
	17	Plaintiff Headwater Research LLC's Amended Infringement Contentions, Headwater Research LLC v. Samsung Electronics Co., 6:23-cv-00103-JRG-RSP (WDTX)	☐
	18		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C	

	19		☐
--	----	--	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	
	Examiner Name	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2024-01-24
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



(11) EP 1 909 463 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.04.2008 Bulletin 2008/15

(51) Int Cl.:
H04L 29/06 (2006.01)

(21) Application number: 08000788.3

(22) Date of filing: 16.10.2006

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI
SK TR
Designated Extension States:
AL BA HR MK RS

(30) Priority: 14.10.2005 KR 20050097241
07.11.2005 KR 20050106213
20.04.2006 KR 20060035949

(62) Document number(s) of the earlier application(s) in
accordance with Art. 76 EPC:
06021650.4 / 1 775 904

(71) Applicant: Samsung Electronics Co., Ltd.
Suwon-si
Gyeonggi-do 443-742 (KR)

(72) Inventors:
• Hwang, Sung-Oh
Suwon-si
Gyeonggi-do (KR)
• Lee, Jong-Hyo
Suwon-si
Gyeonggi-do (KR)

- Lee, Kook-Heui
Suwon-si
Gyeonggi-do (KR)
- Lee, Byung-Rae
Suwon-si
Gyeonggi-do (KR)
- Jung, Bo-Sun
Suwon-si
Gyeonggi-do (KR)
- Lee, Jai-Yong
Suwon-si
Gyeonggi-do (KR)

(74) Representative: Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

Remarks:
This application was filed on 16-01-2008 as a
divisional application to the application mentioned
under INID code 62.

(54) Roaming service method in a mobile broadcasting system, and system thereof

(57) A roaming service method in a mobile broad-
casting system and a system thereof are provided. A ter-
minal receives a service guide from a corresponding vis-
ited service provider (Visited SP) when the terminal
moves to a roaming area. The terminal transmits a roam-
ing request message for requesting a purchase item al-
lowable for individual services to a home service provider
(Home SP) based on the received service guide. Upon

receipt of the roaming request message, the Home SP
negotiates roaming availability and allowable scope for
each individual service with the Visited SP where the
terminal is located, based on the roaming request mes-
sage. The Home SP transmits the roaming availability
and allowable scope for the individual service, negotiated
with the Visited SP, to the terminal.

EP 1 909 463 A1

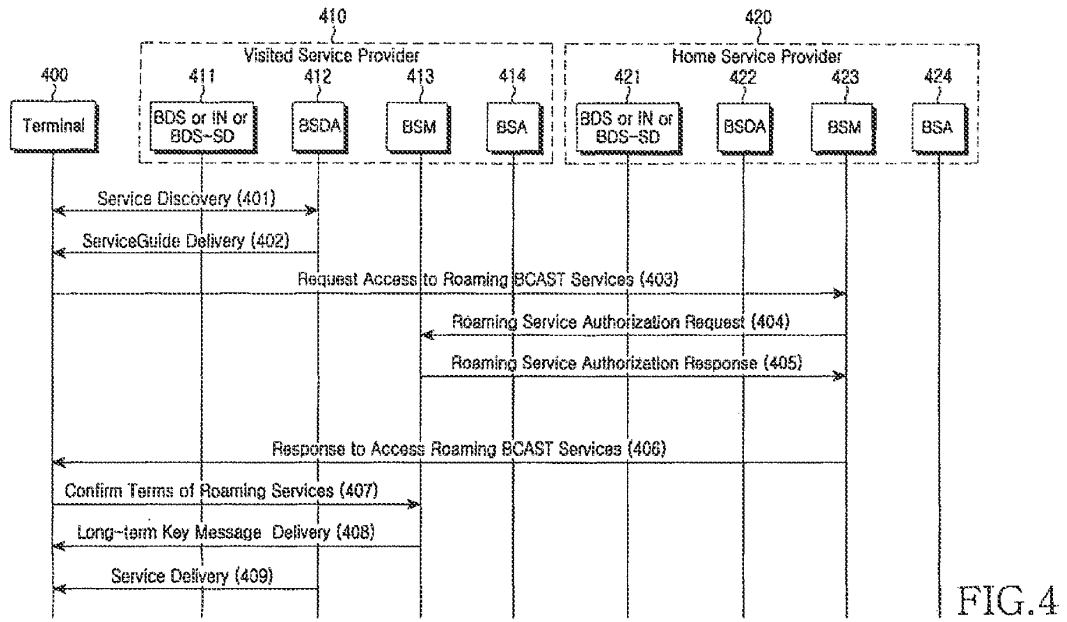


FIG.4

Description

BACKGROUND OF THE INVENTION

5 Field of the Invention:

[0001] The present invention relates generally to a mobile broadcasting system. More particularly, the present invention relates to a roaming service method in a mobile broadcasting system, and a system thereof.

10 Description of the Related Art

[0002] The mobile communication market continuously requires production of new services through recombination or integration of the existing technologies. Today, with the development of communication and broadcast technologies, the conventional broadcasting system or mobile communication system has reached a phase of providing broadcast services through portable terminals (or mobile terminals), such as mobile phone and personal digital assistant (PDA). Due to the latent and actual market needs and an increasing demand for multimedia services, service providers' intended strategies for providing new services such as broadcast service in addition to the existing voice service, and identified interests of Information Technology (IT) companies which are bolstering their mobile communication businesses to meet user's demands, convergence of the mobile communication service and the Internet Protocol (IP) now becomes a mainstream of development of a next generation mobile communication technologies.

[0003] Open Mobile Alliance (OMA), a group for studying the standard for interworking between individual mobile solutions, serves to define various application standards for mobile games and Internet services. Within the OMA working groups, Open Mobile Alliance Browser and Content Mobile Broadcast Sub Working Group (OMA BAC BCAST) currently makes research on technology for providing broadcast services using mobile terminals. A brief description will now be made of the mobile broadcasting system which is under discussion in OMA.

[0004] In a mobile broadcasting system, a mobile terminal desiring to receive a broadcast service should receive so-called service guide information containing description information for the service itself, billing information for the service, and information on a receiving method for the service. The mobile terminal receives the corresponding service using the service guide information.

[0005] A description of conventional technology and novel technology will be made herein based on OMA BCAST technology, which is one of mobile broadcasting technologies, by way of example.

[0006] FIG. 1 is a diagram illustrating a logical structure of an application layer and its lower transport layer for mobile broadcast service, established by a BCAST working group of OMA.

[0007] Logical entities shown in FIG. 1 will first be described in detail. A Content Creation (CC) 101 provides contents for BCAST service, and the contents may include the common broadcast service file, for example, movie, audio and video data. In addition, the Content Creation 101 generates a service guide and provides a BCAST Service Application (BSA) 102 with an attribute for the contents, used for determining a transport bearer where the service is to be transmitted. The BCAST Service Application 102 receives BCAST service data provided from the Content Creation 101, and handles the received data in the form appropriate for providing media encoding, content protection and interaction service. Further, the BCAST Service Application 102 provides an attribute for the contents provided from the Content Creation 101 to a BCAST Service Distribution/Adaptation (BSDA) 103 and a BCAST Subscription Management (BSM) 104.

[0008] The BCAST Service Distribution/Adaptation 103 performs such operations as file/streaming transmission, service collection, service protection, service guide generation/delivery, and service notification, using BCAST service data provided from the BCAST Service Application 102. In addition, the BCAST Service Distribution/Adaptation 103 adapts the service such that it should be suitable for a Broadcast Distribution System (BDS) 112.

[0009] The BCAST Subscription Management 104 prescribes such service as a subscription and billing-related function for a BCAST service user, prescribes information used for the BCAST service, and manages a terminal receiving the BCAST service by hardware or software.

[0010] A Terminal 105 receives such program resource information as a content/service guide and content protection, and provides a broadcast service to a user. A BDS Service Distribution (BDS-SD) 111 transmits a mobile broadcast service to a plurality of terminals through mutual communication with the Broadcast Distribution System 112 and an Interaction Network (IN) 113.

[0011] The Broadcast Distribution System 112 transmits mobile broadcast service through a broadcast channel. For example, the mobile broadcast service can include Multimedia Broadcast Multicast Service (MBMS) of 3rd Generation Project Partnership (3GPP), Broadcast Multicast Service (BCMCS) of 3rd Generation Project Partnership 2 (3GPP2), and DVB-Handheld (DVB-H) or Internet Protocol (IP)-based broadcast/communication network of Digital Video Broadcasting (DVB). The Interaction Network 113 provides an interaction channel. For example, the Interaction Network 113 can be a cellular network.

[0012] A description will now be made of reference points, which are connection paths between the logical entities. The reference point can have a plurality of interfaces according to purpose, and such an interface is used for communication between more than two logical entities for a specific purpose. A message format and protocol for this is applied.

[0013] BCAST-1 121 is a transmission path of content and content attribute, and BCAST-2 122 is a transmission path of content-protected or content-unprotected BCAST service, attribute of the BCAST service, and content attribute.

[0014] BCAST-3 123 is a transmission path of attribute of BCAST service, attribute of content, user preference and subscription information, user request, and response to the request. BCAST-4 124 is a transmission path of notification message, attribute used for service guide, and key used for content protection and service protection.

[0015] BCAST-5 125 is a transmission path of protected BCAST service, unprotected BCAST service, content-protected BCAST service, content-unprotected BCAST service, BCAST service attribute, content attribute, notification, service guide, security material such as Digital Right Management (DRM) Right Object (RO) and key value used for BCAST service protection, and all data and signals transmitted through a broadcast channel.

[0016] BCAST-6 126 is a transmission path of protected BCAST service, unprotected BCAST service, content-protected BCAST service, content-unprotected BCAST service, BCAST service attribute, content attribute, notification, service guide, security material such as DRM RO and key value used for BCAST service protection, and all data and signals transmitted through an interaction channel.

[0017] BCAST-7 127 is a transmission path of service provisioning, subscription information, device management, and user preference information transmitted through an interaction channel of control information related to reception of security material such as DRM RO and key value used for BCAST service protection.

[0018] BCAST-8 128 is a transmission path through which user data for BCAST service is interacted. BDS-1 129 is a transmission path of protected BCAST service, unprotected BCAST service, BCAST service attribute, content attribute, notification, service guide, and security material such as DRM RO and key value used for BCAST service protection.

[0019] BDS-2 130 is a transmission path of service provisioning, subscription information, device management, and security material such as DRM RO and key value used for BCAST service protection. X-1 131 is a reference point between the BDS Service Distribution 111 and the Broadcast Distribution System 112. X-2 132 is a reference point between the BDS Service Distribution 111 and the Interaction Network 113. X-3 133 is a reference point between the Broadcast Distribution System 112 and the Terminal 105. X-4 134 is a reference point between the BDS Service Distribution 111 and the Terminal 105 via the broadcast channel. X-5 135 is a reference point between the BDS Service Distribution 111 and the Terminal 105 via the interaction channel. X-6 136 is a reference point between the Interaction Network 113 and the Terminal 105.

[0020] FIG. 2 is a diagram illustrating a structure of a service guide used for receiving a broadcast service in a general mobile broadcasting system. This structure is proposed in OMA BAC BCAST to provide broadcast service to a mobile terminal. One service guide is composed of a plurality of fragments each having its own purpose, and the fragments are classified into 4 groups according to use, as shown in FIG. 2.

[0021] FIG. 2 illustrates an exemplary service guide composed of an Administrative group 200, a Provisioning group 210, a Core group 220, and an Access group 230. In FIG. 2, a solid line connecting the fragments means mutual reference between the fragments.

[0022] The Administrative group 200, a group for providing basic information needed by a mobile terminal to receive a service guide, includes a Service Guide Context fragment 201 and a Service Guide Delivery Descriptor fragment 202.

[0023] The Service Guide Context fragment 201 provides a service guide identifier (ID), identification information of the service provider that generated and transmitted the service guide, and the entire information on the service guide. The Service Guide Delivery Descriptor fragment 202 provides a channel capable of receiving a plurality of service guide fragments, scheduling information, and update information to a mobile terminal so that the mobile terminal may receive only the necessary service guide at an appropriate time.

[0024] The Provisioning group 210, a group for providing charging information for service reception, includes a Purchase Item fragment 211, a Purchase Data fragment 212, and a Purchase Channel fragment 213. The Purchase Item fragment 211 provides charging information for a service or a service bundle, the Purchase Data fragment 212 indicates actual price information for a purchase item, and the Purchase Channel fragment 213 provides information on the system where the service user can actually purchase the service, and a payment method.

[0025] The Core group 220, a group for providing information on the service itself, includes a Service fragment 221, a Schedule fragment 222, and a Content fragment 223. The Service fragment 221 provides a description of the service itself that the user will receive, and also provides information indicating with which content the service can be configured. The Schedule fragment 222 provides information on the time at which the service can be provided and used. The Content fragment 223 provides information on a plurality of contents constituting the service.

[0026] The Access group 230 includes an Access fragment 231 and a Session Description fragment 232, and provides service access information indicating how to receive the services provided through the Core group 220, and detailed information on the session in which the contents constituting the corresponding service are transmitted to allow the mobile terminal to access the corresponding service.

[0027] The Access fragment 231 provides a plurality of access methods for one service to the mobile terminal, thereby providing a method capable of accessing various additional services based on one service. The Session Description fragment 232 provides session information for the service defined in one access fragment. In addition, the service guide information, as shown in FIG. 2, can further include a Preview Data fragment 224 that provides preview and icon for the service and content in addition to the foregoing four fragments.

[0028] FIG. 3 is a diagram illustrating a roaming procedure performed when a mobile broadcasting terminal desires to receive broadcast service not in a service area of its Home Network (Home N/W) 310, but in a service area of a Visited Network (Visited N/W) 320 in OMA BCAST. Before a description of each step in the roaming procedure is given, each entity of FIG. 3 will first be described.

[0029] BCAST Service Applications (BSAs) 311 and 321 in the Home N/W 310 and the Visited N/W 320 are equal in function to the BCAST Service Application 102 of FIG. 1, so they are separately shown to differentiate the BSA in the Home N/W 310 from the BSA in the Visited N/W 320 during roaming. Similarly, BCAST Subscription Managements (BSMs) 312 and 322 have the same function as that of the BCAST Subscription Management 104 of FIG. 1. BCAST Service Distribution Adaptations (BSDAs) 313 and 323 have the same function as that of the BCAST Service Distribution/Adaptation 103 of FIG. 1, and group entities 314 and 324, each composed of BDS Service Distribution (BDS-SD), BCAST Distribution System (BDS) and/or Interaction Network (IN), have the same function as the group entity of the BDS-SD 111, the BDS 112 and/or the IN 113 of FIG. 1. A Terminal 330 has the same function as that of the Terminal 105 of FIG. 1. Each step in the roaming procedure will now be described.

[0030] In step 301, a user requests a BCAST roaming service in its Home N/W 310, and then moves to the Visited N/W 320. A procedure for roaming from the Home N/W 310 to the Visited N/W 320 should be performed outside the BCAST area in the lower layers 313 and 323. In step 302, the Terminal 330 automatically receives a service guide from the Visited N/W 320 to which it is roaming, without connection to the Home N/W 310. In step 303, upon receiving the service guide, the Terminal 330 sends a request for Rights Object for a particular BCAST service desired by the user to the BSM 322 of the Visited N/W 320. In step 304, the BSM 322 of the Visited N/W 320 acquires authorization for user roaming to the BSM 312 of the Home N/W 310. In step 305, the BSM 322 delivers the Right Object requested by the Terminal 330 in step 303 to the Terminal 330 via the BSM 321 of the Visited N/W 320. After receiving the Right Object in step 305, the Terminal 330 receives the BCAST service via the BSDA 323 of the Visited N/W 320 in step 306. Finally, in step 307, the Visited N/W 320 generates charging information and delivers the charging information to the Home N/W 310, which is outside the BCAST standard, so a description thereof will not be given.

[0031] As described in FIG. 3, BCAST currently presents the roaming procedure. Although there is a need for a message for communication between the entities and its message format in order to actually make the roaming possible, a message for communication between the entities and its message format, they are not presented. In the mobile broadcast service where several service providers may exist, in order for user terminals to freely roam and receive the service, the message flow between BCAST service entities should be specifically presented. In the current roaming procedure, when a user has performed roaming, the procedure is achieved without notification for charging information. However, when roaming occurs actually, the charging system is different from that of the Home N/W 310, which has been used by the user, and the user is not also charged according to the charge in the service guide of the Visited N/W 320, which was received while in roaming. Because of this, there is a need for a step capable of providing information on a change in the charge to the user and allowing the user to determine whether he/she will use the roaming service. In addition, in order to make the roaming procedure possible, a request for the roaming service should be previously sent to the Home N/W 310. However, because such a situation is not always possible, the roaming should be possible even after the terminal moves the area. It is assumed in the roaming procedure of FIG. 3 that the scheme used for deciphering the enciphered content or service received in step 305 is OMA DRM 2.0. Actually, the roaming procedure should be updated such that the content or service can be enciphered/deciphered even by the schemes other than the OMA DRM 2.0. Accordingly, there is a need for an improved method for supporting a roaming service in the mobile broadcasting system.

SUMMARY OF THE INVENTION

[0032] An aspect of exemplary embodiments of the present invention is to address at least the above problems and/or disadvantages and to provide at least the advantages described below. Accordingly, an aspect of exemplary embodiments of the present invention is to provide a roaming service method in a mobile broadcasting system, and a system thereof.

[0033] It is another aspect of exemplary embodiments of the present invention to provide a roaming service method capable of supporting various charging systems in a mobile broadcasting system, and a system thereof.

[0034] It is further another aspect of exemplary embodiments of the present invention to provide a roaming service method for supporting various enciphering schemes in a mobile broadcasting system, and a system thereof.

[0035] According to one aspect of exemplary embodiments of the present invention, there is provided a roaming service method in a mobile broadcasting system, in which a service guide from a corresponding visited service provider

(Visited SP) is received by the terminal when the terminal moves to a roaming area, a roaming request message for requesting a purchase item allowable for each individual service is transmitted by the terminal to a home service provider (Home SP) based on the received service guide, upon receipt of the roaming request message, roaming availability and allowable scope for each individual service with the Visited SP where the terminal is located is negotiated by the Home SP, based on the roaming request message, the roaming availability and allowable scope for each individual service, negotiated with the Visited SP, is transmitted by the Home SP to the terminal, agreement/disagreement on the allowable scope for each individual service is transmitted by the terminal to the Visited SP, and if the terminal agrees, an enciphering key for receiving the agreed service is transmitted by the Visited SP.

[0036] In an exemplary implementation, the roaming request message further includes an allowability request of a particular service selected by the terminal.

[0037] In another exemplary implementation, the negotiating of the roaming availability and allowable scope comprises transmitting, by the Home SP, a message including a subscription type of the terminal to the Visited SP, for roaming registration; and determining, by the Visited SP, roaming availability and allowable scope for each individual service based on the subscription type, and transmitting the result to the Home SP.

[0038] In still another exemplary implementation, the enciphering key is a long-term key.

[0039] According to another aspect of exemplary embodiments of the present invention, there is provided a roaming service method in a mobile broadcasting system, in which a service guide from a corresponding visited service provider (Visited SP) is received by a terminal when the terminal moves to a roaming area, a roaming request message for requesting a purchase item allowable for each individual service is transmitted by the terminal to the Visited SP based on the received service guide, upon receipt of the roaming request message, whether a roaming service of the terminal is authorized from a home service provider (Home SP) for which the terminal has subscribed, based on the roaming request message is determined by the Visited SP, availability of the roaming service of the terminal and an allowable scope for each individual roaming service is verified by the Visited SP, and the result is transmitted to the terminal, agreement/disagreement on the allowable scope for each individual service is transmitted by the terminal to the Visited SP, and if the terminal agrees, an enciphering key for receiving the agreed service is transmitted by the Visited SP.

[0040] In an exemplary implementation, the transmitted of the roaming request message further comprises including an allowability request of a service selected by the terminal in the roaming request message.

[0041] In another exemplary implementation, the determining of whether a roaming service of the terminal is authorized comprises transmitting, by the Visited SP, a message including a subscription type of the terminal to the Home SP, for roaming registration; and determining, by the Home SP, roaming availability based on the subscription type, and transmitting the determined roaming availability to the Home SP.

[0042] According to a further aspect of exemplary embodiments of the present invention, there is provided a mobile broadcasting system comprising a home service provider (Home SP) for, upon receipt of a roaming request message from a terminal, negotiating roaming availability and allowable scope for each individual roaming service with a visited service provider (Visited SP) where the terminal is located, based on the roaming request message, the Visited SP for transmitting the negotiated roaming availability and allowable scope for each individual roaming service to the terminal, and the terminal for verifying the received roaming availability and allowable scope for each individual roaming service, and receiving an enciphering key from the Home SP or the Visited SP.

[0043] In an exemplary implementation, the terminal further includes an allowability request of a service selected by the terminal in the roaming request message.

[0044] In another exemplary implementation, the enciphering key is a long-term key.

[0045] According to yet another aspect of exemplary embodiments of the present invention, there is provided a mobile broadcasting system comprising a visited service provider (Visited SP) for, upon receipt of a roaming request message from a terminal, inquiring of a home service provider (Home SP) for which the terminal has subscribed, regarding availability of the roaming service, based on the roaming request message, checking the roaming availability and allowable scope for each individual roaming service, and transmitting the result to the terminal, the Home SP for, upon receipt of a request for the roaming service of the terminal from the Visited SP, determining whether to authorize the roaming service of the terminal and transmitting the result to the Visited SP, and the terminal for checking the roaming availability and allowable scope for each individual roaming service, and receiving an enciphering key from the Home SP or the Visited SP.

[0046] In an exemplary implementation, the terminal further includes an allowability request of a service selected by the terminal in the roaming request message before transmission.

[0047] According to still another aspect of exemplary embodiments of the present invention, there is provided a roaming service method in a terminal of a mobile broadcasting system, in which a roaming request message for requesting a purchase item allowable for each individual service is transmitted to its home service provider (Home SP) or a visited service provider (Visited SP) based on a service guide received from the Visited SP when the terminal moves to a roaming area, a roaming response message from the Home SP or the Visited SP is received, roaming availability and allowable scope for each individual service is verified, and agreement/disagreement is transmitted to the Home SP or

the Visited SP, and if the checked roaming condition is agreed, an enciphering key is received from the Home SP or the Visited SP.

[0048] In an exemplary implementation, the terminal further includes an allowability request of a service selected by a user in the roaming request message.

5 **[0049]** In another exemplary implementation, the roaming response message further includes charging information for a roaming service to the terminal.

[0050] According to still another aspect of exemplary embodiments of the present invention, there is provided a terminal in a mobile broadcasting system, in which a controller generates a roaming request message for requesting a purchase item allowable for each individual service based on a service guide received from a corresponding visited service provider (Visited SP), when the terminal moves to a roaming area, and deciphering a response message to the roaming request, and a transceiver transmits the generated roaming request message to a home service provider (Home SP) or the Visited SP, and receives a roaming response message from the Home SP or the Visited SP and transmits the received roaming response message to the controller.

10 **[0051]** In an exemplary implementation, the controller further includes an allowability request of a service selected by a user in the roaming request message.

15 **[0052]** In another exemplary implementation, the roaming response message further includes charging information for a roaming service to the terminal.

BRIEF DESCRIPTION OF THE DRAWINGS

20 **[0053]** The above and other objects, features and advantages of certain exemplary embodiments of the present invention will be more apparent from the following detailed description taken in conjunction with the accompanying drawings, in which:

25 FIG. 1 is a diagram illustrating a functional structure of a mobile broadcasting system;
 FIG. 2 is a diagram illustrating a structure of a service guide used for receiving a broadcast service in a general mobile broadcasting system;
 FIG. 3 is a diagram illustrating a conventional roaming procedure in OMA BCAST;
 30 FIG. 4 is a signaling diagram illustrating a roaming procedure according to an exemplary embodiment of the present invention;
 FIG. 5 is a flowchart illustrating an operation of a BSM of a Visited SP according to an exemplary embodiment of the present invention;
 FIG. 6 is a flowchart illustrating an operation of a BSM of a Home SP according to an exemplary embodiment of the present invention;
 35 FIG. 7 is a flowchart illustrating an operation of a Terminal according to an exemplary embodiment of the present invention;
 FIG. 8 is a signaling diagram illustrating a roaming procedure according to an exemplary embodiment of the present invention;
 FIG. 9 is a flowchart illustrating an operation of a BSM of a Visited SP according to an exemplary embodiment of the present invention;
 40 FIG. 10 is a flowchart illustrating an operation of a BSM of a Home SP according to an exemplary embodiment of the present invention;
 FIG. 11 is a flowchart illustrating an operation of a Terminal according to an exemplary embodiment of the present invention;
 45 FIG. 12 is a diagram illustrating an exemplary protocol stack usable for communication between BSMs according to an exemplary embodiment of the present invention;
 FIG. 13 is a signaling diagram illustrating a roaming procedure according to an exemplary embodiment of the present invention;
 FIG. 14 is a flowchart illustrating an operation of a BSM of a Visited SP according to an exemplary embodiment of the present invention;
 50 FIGs. 15A and 15B are flowcharts illustrating an operation of a BSM of a Home SP according to an exemplary embodiment of the present invention;
 FIG. 16 is a flowchart illustrating an operation of a Terminal according to an exemplary embodiment of the present invention;
 55 FIG. 17 is a signaling diagram illustrating a purchase item list request procedure for roaming according to an exemplary embodiment of the present invention;
 FIG. 18 is a flowchart illustrating an operation of a BSM of a Visited SP according to an exemplary embodiment of the present invention;

FIG. 19 is a diagram illustrating an operation of a BSM of a Home SP according to an exemplary embodiment of the present invention;

FIG. 20 is a flowchart illustrating an operation of a Terminal according to an exemplary embodiment of the present invention;

5 FIG. 21 is a signaling diagram illustrating a purchase item list request procedure for roaming according to an exemplary embodiment of the present invention;

FIG. 22 is a flowchart illustrating an operation of a BSM of a Visited SP according to an exemplary embodiment of the present invention;

10 FIG. 23 is a flowchart illustrating an operation of a BSM of a Home SP according to an exemplary embodiment of the present invention; and

FIG. 24 is a flowchart illustrating an operation of a Terminal according to an exemplary embodiment of the present invention.

15 **[0054]** Throughout the drawings, the same drawing reference numerals will be understood to refer to the same elements, features and structures.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

20 **[0055]** The matters defined in the description such as a detailed construction and elements are provided to assist in a comprehensive understanding of exemplary embodiments of the invention. Accordingly, those of ordinary skill in the art will recognize that various changes and modifications of the embodiments described herein can be made without departing from the scope and spirit of the invention. Also, descriptions of well-known functions and constructions are omitted for clarity and conciseness.

25 **[0056]** In the following description, the representative exemplary embodiments of the present invention will be presented. For convenience, although names of the entities defined in 3rd Generation Partnership Project (3GPP) which is a standard group for asynchronous mobile communication will be used as names of the entities defined in BCAST of Open Mobile Alliance (OMA) which is a standard group of an application of a mobile terminal, the standards and names will not limit the scope of the present invention, and can also be applied to the systems having the similar technical background. Actually, in the BCAST structure, the Home N/W 310 and the Visited N/W 320 of FIG. 3 should be replaced
30 by a Home Service Provider (Home SP) and a Visited Service Provider (Visited SP).

[0057] Before a description of the BCAST roaming procedure according to an exemplary embodiment of the present invention is given, the information necessary for the procedure will be described.

35 **[0058]** Table 1 to Table 4 below show items stored in the Service Guide Context fragment 201 described in FIG. 2. Table 1 to Table 4 are divided from one table, for convenience, and those are described in detail in Korean Patent Application No. P2005-94675, entitled Method and Apparatus for Transmitting and Receiving Service Guide Context in a Mobile Broadcasting System. Exemplary embodiments of the present invention uses partial information provided in Table 1 to Table 4, so a description of the unused items will be omitted for clarity and conciseness. Therefore, for a detailed description of Table 1 to Table 4, refer to the earlier filed application.

40 Table 1

Name	Type	Category	Cardinality	Description
Service GuideContext			..N	Identifies the SGDD to the terminal. Each Service Providers may have their own announcement channel. ServiceGuideContext gives an session information of announcement channel which contains SGDDs. Contains the following elements: ServiceGuideInfo
Service GuideInfo	1		..N	Specifies Service Guide Information. Contains the following attributes: SGVersion BSDAId

(continued)

Name	Type	Category	Cardinality	Description
				Contains the following elements: Name ServiceProvider Broadcast_area SGAnnouncement SGFragmentsList
SGVersion				Version of Service Guide. The newer version overrides the older one as soon as it has been received
BSDAid				Identifier of BSDA system which distribute and aggregate service guide fragments.
Release Time				

Table 2

Name	2		..N	Name of Service Guide, possibly in multiple languages. The language is expressed using built-in XML attribute xml:lang with this elements
Service Provider	2			Specifies an information of service provider who deliver the service guides Contains the following attributes: ProviderURI ProviderName
Provider URI				Specifies a service provider's URI which is globally unique. This URI is registered by ICANN.
Provider Name				Specifies the Service Providers' name.
Broadcast_area	2		..N	The broadcast area to distribute contents (as specified in the [OMA MLP] with modifications) Sub-elements: Shape cc name__area zip_code
Shape	3		..1	Shapes used to represent a geographic area that describes (as specified in the [OMA MLP])
Cc	3		..1	Country code, 1-3 digits e.g. 355 for Albania (as specified in the [OMA MLP])
name__area	3		..1	Geopolitical name of area such as 'Seoul' (as specified in the [OMA MLP])
zip_code	3		..1	Zip code

Table 3

SGAnnouncement	2			Specifies an information of Service Guide Announcement Session. Contains the following elements: AnnouncementSession
----------------	---	--	--	--

(continued)

				SGDDInfo
5	AnnouncementSession	3		The pointer to the Announcement Channel delivering ServiceGuideDeliveryDescriptor. Contains the following attributes: SrcIPAddress DestIPAddress PortNumber SessionID
10	SrcIP Address			Source IP address of the announcement channel which is the FLUTE session
15	DestIPAddress			Destination IP address of the announcement channel which is the FLUTE session
	PortNumber		..1	Destination port of the announcement channel which is the FLUTE session
20	SessionID			Identifier of the announcement session
	SGDDInfo	3		Specifies the SGDD information Contains the following attributes: NumberOfSGDDs ListeningPeriod
25	ListeningPeriod		..1	Time Duration for listening of SGDD Delivery by Terminal

Table 4

30	SGFragmentsList	2		Specifies the total lists of Fragments which composed the service guide. Contains the following elements: ServiceFragmentList ScheduleFragmentList ContentFragmentList PurchaseItemFragmentList PurchaseDataFragmentList PurchaseChannelFragmentList AccessFragmentList
35	Service FragmentList	3		Specifies the total list of Service Fragments
40	FragmentID	4	..N	Service Fragments IDs
	ScheduleFragmentList	3		Specifies the total list of Schedule Fragments
	FragmentID	4	..N	Schedule Fragments IDs
45	Content FragmentTable	3		Specifies the total list of Content Fragments
	FragmentID	4	..N	Content Fragments IDs
	PurchaseItemFragmentList	3		Specifies the total list of PurchaseItem Fragments
	FragmentID	4	..N	PurchaseItem Fragments IDs
50	PurchaseDataFragmentList	3		Specifies the total list of PurchaseData Fragments
55	FragmentID	4	..N	PurchaseData Fragments IDs

(continued)

PurchaseChannelFragmentList	3			Specifies the total list of PurchaseChannel Fragments
FragmentID	4		..N	Purchase Channel Fragments IDs
AccessFragmentList	3			Specifies the total list of Access Fragments
FragmentID	4		..N	Access Fragments IDs

[0059] Referring to Table 1 to Table 4, 'Name' indicates names of element values and attribute values constituting a corresponding message. 'Type' indicates whether the corresponding name corresponds to an element value or an attribute value. The element value has values of E1, E2, E3 and E4. E1 means an upper element value for the whole message, E2 indicates a sub-element value of E1, E3 indicates a sub-element value of E2, and E4 indicates a sub-element value of E3. The attribute value is indicated by A, and A indicates an attribute value of the corresponding element. For example, A under E1 indicates an attribute value of E1. 'Category' is used for indicating whether a corresponding element value or attribute value is mandatory, and has a value M if the value is mandatory, and a value O if the value is optional. 'Cardinality' indicates relations between the elements, and has values of '0', '0..1', '1', '0..n', '1..n', where "0" means an optional relation, "1" means a mandatory relation, and 'n' means the possibility of having a plurality of values. For example, '0..n' means the possibility that there is no corresponding element value or there are n corresponding element values. 'Description' defines the meaning of the corresponding element or attribute value.

[0060] As described in FIG. 2, the Service Guide Context fragment 201 provides overall information on the service guide and, in particular, has an attribute BSDAid and an element ServiceProvider. The attribute BSDAid is an identifier of the BSDA 103 for delivering the BCAST service in the corresponding area. The element ServiceProvider is composed of attributes of ProviderURL and ProviderName, and these are identifier information of the service provider that provides the BCAST service in the corresponding area. That is, the Terminal 105 can acquire information on the service provider and deliverer in the place where it is receiving the service through the information stored in the BSDAid and the ServiceProvider.

[0061] Table 5 to Table 7 below show items stored in the Purchase Item fragment 211. Table 5 to Table 7 are divided from one table, for convenience, and those are described in detail in the OMA standard document. Exemplary embodiments of the present invention uses partial information provided in Table 5 to Table 7, so a description of the unused items will be omitted for clarity and conciseness. For a detailed description of Table 5 to Table 7, refer to the documents in the OMA web site http://www.openmobilealliance.org/ftp/Public_documents/BACBCAST/Permanent_documents/OMA-TS-TS-BCAST_ServiceGuide-V1.0.0-20050930-D.zip, which are incorporated by reference. The reference documents were the newest edition as of the filing date of this application, and if there is any update in the documents in the future, the updated edition will be applied.

Table 5

Name	Type	Category	Cardinality	Description
PurchaseItem			..N	PurchaseItem fragment Contains the following attributes: id version validFrom validTo Weight Contains the following sub-elements: ExtensionURL ServiceIDRef ScheduleIDRef ContentIDRef Name Description ParentalRating PurchaseDataIDRef
id				ID of the PurchaseItem fragment, globally unique

(continued)

Name	Type	Category	Cardinality	Description
version				Version of this fragment. The newer version overrides the older one as soon as it has been received.
validFrom			..1	The first moment when this fragment is valid. If not given, the validity is assumed to have started at some time in the past

Table 6

validTo			..1	The last moment when this fragment is valid. If not given, the validity is assumed to end in undefined time in the future.
Weight		O/TM		Intended order of display of this purchase item relative to other purchase items as seen by the end user. The order of display is by increasing Weight value (i.e., purchase item with lowest Weight is displayed first).
ExtensionURL	1		..N	URL containing additional information related to this fragment in a web page. The terminal can fetch further information by accessing this URL.
ServiceIDRef	1		..N	References to the Service fragments which belong to this PurchaseItem. Note: a Service fragment can be referenced by multiple PurchaseItems.
ScheduleIDRef	1		..N	References to the Schedule fragments which belong to this Purchase Item. Note: a Schedule fragment can be referenced by multiple PurchaseItems.
ContentIDRef	1		..N	References to the Content fragments which belong to this PurchaseItem. Note: a Content fragment can be referenced by multiple PurchaseItems.
Name	1		..N	Name of the PurchaseItem, possibly in multiple languages. The language is expressed using built-in XML attribute xml:lang with this element.

Table 7

Description	1	O/TM	..N	Description of the purchase item, possibly in multiple languages. The language is expressed using built-in XML attribute xml:lang with this element.
ParentalRating	1		..1	This determines the age limit for service purchase, not the age limit of the actual service consumption. The allowed values are those defined in the ParentalRating Descriptor of the EIT table (cf. ETSI EN 300 468)
PurchaseDataIDRef	1		..N	References to PurchaseData fragment, which belongs to this Purchase Item.
<proprietary elements>	1 or lower		..N	Any number of proprietary or application-specific elements that are not defined in this specification.

[0062] As described in FIG. 2, the Purchase Item fragment 211 provides charging information for a service or a service

bundle, and an attribute 'id' of Table 5 to Table 7 indicates an identifier ID of the service indicated by the Purchase Item fragment 211.

[0063] Table 8 to Table 10 below show items stored in the Purchase Channel fragment 213. Table 8 to Table 10 are divided from one table, for convenience, and those are described in detail in the OMA standard document. Exemplary embodiments of the present invention uses partial information provided in Table 8 to Table 10, so a description of the unused items will be omitted for clarity and conciseness. For a detailed description of Table 8 to Table 10, refer to the documents in the OMA web site [http://www.openmobilealliance.org/ftp/Public documentsBACBCAST/Permanent documents/OMA-TS-TS-BCAST ServiceGuide-V1.0.0-20050930-D.zip](http://www.openmobilealliance.org/ftp/Public%20documents/BACBCAST/Permanent%20documents/OMA-TS-TS-BCAST%20ServiceGuide-V1.0.0-20050930-D.zip), which are incorporated by reference. The reference documents were the newest edition as of the filing date of this application, and if there is any update in the documents in the future, the updated edition will be applied.

Table 8

Name	Type	Category	Cardinality	Description
PurchaseChannel			..N	PurchaseChannel fragment Contains the following attributes: id version validFrom validTo LocalFlag RightsIssuerURI Selector Contains the following sub-elements: ExtensionURL Name PortalURL Description Connection ContactInfo
id				ID of the PurchaseChannel fragment, globally unique
version				Version of this fragment. The newer version overrides the older one as soon as it has been received.
validFrom			..1	The first moment when this fragment is valid. If not given, the validity is assumed to have started at some time in the past
validTo			..1	The last moment when this fragment is valid. If not given, the validity is assumed to end in undefined time in the future.

Table 9

LocalFlag				If true, indicates that the BSM advertises the availability and purchase information completely in the service guide
RightsIssuerURI		O/O		ID of the rights issuer associated with the BSM (needed to allow unconnected devices to identify the RI service that may be operated by their Home BSM). If the service protection or content protection system is based on OMA DRM2.0, RightsIssuerURI SHALL be specified.
Selector				Allows a terminal to determine which purchase channel to use, among the purchase channels that are announced in the SG.

(continued)

				Attributes: type (e.g. possible value: "SIMCode") Note: Purchase channel needs to be provided by the BCAST Service Provider.
5	Extension URL	1	..N	URL containing additional information related to this fragment in a web page. The terminal can fetch further information by accessing this URL.
10	Name	1	..N	Name of the Purchase Channel, possibly in multiple languages. The language is expressed using built-in XML attribute xml:lang with this element.
	PortalURL	1	..1	URL for the BSM, on which all purchase transactions can be made
15	Description	1	..N	Description of the purchase channel, possibly in multiple languages. The language is expressed using built-in XML attribute xml:lang with this element.

Table 10

20	Connection	1	..N	Allows a terminal to construct a purchase request and send it to the purchase channel. In case multiple connection options are specified, it is up to the terminal to choose, e.g. to use IP (over GPRS), with SMS as a fallback option. Contains the following sub-elements: PurchaseURL
25	Purchase URL	2	..N	The URL to which the purchase request should be addressed. Contains the following attribute: Bearer
30	Bearer			Bearer supporting this purchase channel
35	ContactInfo	1	..1	A text string that indicates to a user how to contact a BSM to initiate an out-of-band purchase transaction (e.g. phone number, URL etc)
40	<proprietary elements>	1 or lower	..N	Any number of proprietary or application-specific elements that are not defined in this specification.

[0064] As described in FIG. 2, the Purchase Channel fragment 213 provides information indicating which entity the service user should access to actually purchase the service or service bundle indicated by the Purchase Item fragment 211. An element PortalURL in Table 8 to Table 10 has a URL of the BSM 104 that performs purchase management. As described in FIG. 1, the BSM 104 performs user management as well as the purchase management.

[0065] The elements and attributes mentioned for the roaming in Table 1 to Table 10 are listed in Table 11, and usage of the elements and attributes during the roaming will be described hereinbelow.

Table 11

50	BSDAId			Identifier of BSDA system which distribute and aggregate service guide fragments.
55	ServiceProvider	2		Specifies an information of service provider who deliver the service guides Contains the following attributes: ProviderURI ProviderName

(continued)

ProviderURI				Specifies a service provider's URI which is globally unique. This URI is registered by ICANN.
ProviderName				Specifies the Service Providers' name.
id				ID of the PurchaseItem fragment, globally unique
PortalURL	1		..1	URL for the BSM, on which all purchase transactions can be made

- 10 **[0066]** BSDAid is an identifier of the BSDA 103, through which the entity from which the service is provided can be found. If the Terminal 105 is located in the Home SP, the BSDAid is a URL of the BSDA of its service provider. If the Terminal 105 is located in the Visited SP after roaming, the BSDAid is a URL of the BSDA of the service provider in the roaming area. Attributes ProviderURI and ProviderName of the element ServiceProvider indicate unique URL information and name of the service provider, respectively. When the Terminal 105 is located in the Home SP, the ProviderURI is a URL of its service provider, and when the Terminal 105 is located in the Visited SP after roaming, the ProviderURI is a URL of the service provider in the roaming area. The Terminal 105 uses the BSDAid, ProviderURI, and ProviderName during roaming in order to identify the service provider when it makes roaming registration in the Visited SP and the Home SP. For example, the BSDAid is needed to determine in which area the roaming terminal desires to receive the service when one service provider provides the BCAST service in several areas. The attribute 'id' is an identifier of the service that the roaming user desires to receive in the roaming area, and is used when the roaming service is registered. Finally, the PortalURL is used for acquiring information on the BSM 104 of the Home SP and the Visited SP, which performs and manages roaming registration. A roaming service registration request is actually delivered to the position stored in the PortalURL.
- 15 **[0067]** There is a need for a unique identifier of the Terminal 105 that requests the service, in addition to the information provided by the elements or attributes mentioned in Table 11. The unique identifier of the terminal is an identifier that the terminal basically has. In addition, as to the information of the items mentioned in Table 11, the information related to the Home SP of the roaming terminal is fully known by the terminal through the service guide of the Home SP. The attributes and elements mentioned to be needed for roaming in Table 11 are exemplary attributes and elements made based on the BCAST standard document. Therefore, if the BCAST standard document is updated, names of the attributes and elements affecting the present invention can also be changed according thereto.
- 20 **[0068]** Next, a description will be made of an exemplary roaming procedure according to an exemplary embodiment of the present invention. The roaming procedure can be achieved with two methods. The first method is performed in the case where when the terminal, after roaming, first desires to make roaming request registration in the Visited SP, the registration-requested entity is the BSM of the Home SP. The second method is performed in the case where when the terminal, after roaming, first desires to make roaming request registration in the Visited SP, the registration-requested entity is the BSM of the Visited SP. A detailed description of each method will be made hereinbelow.
- 25 **[0069]** Before a description of each method is given, FIG. 12 will be described.
- 30 **[0070]** FIG. 12 is a diagram illustrating an exemplary protocol stack usable for communication between BSMs 104 according to an exemplary embodiment of the present invention. Although a HTTP protocol of FIG. 12 is a protocol originally designed to transmit web pages, it is now used as a protocol for transmitting a variety of information. Also, the messages for roaming, to be defined in an exemplary embodiment of the present invention, are generated, and those are transmitted using the HTTP protocol. HTTP-encapsulated roaming messages are encapsulated according to the transport layer protocol such as a lower TCP protocol. The TCP protocol is given by way of example, because it is a typical protocol for the transport layer. For security or efficiency, another transport layer protocol can also be used. If the TCP encapsulation is completed, IP is used as a network layer protocol. Because OMA BCAST is IP-based mobile broadcast service, IP should be used as the network layer protocol. However, for security, IPsec can be used together with IP. If a transmitting BSM transmits a message to a receiving BSM according to the above procedure, the receiving BSM can acquire the transmitted actual message by decapsulating the message in the reverse order of the above procedure. In communication between the BSMs according to an exemplary embodiment of the present invention, message exchange will be achieved using the protocol stack of FIG. 12.
- 35 **[0071]** FIG. 4 is a signaling diagram illustrating a roaming procedure according to an exemplary embodiment of the present invention. Before a description of each step in the roaming procedure is given, each entity of FIG. 4 will be described. BSAs 424 and 414 in a Home SP 420 and a Visited SP 410 are equal in function to the BSA 102 of FIG. 1, so they are separately shown to differentiate the BSA in the Home SP 420 from the BSA in the Visited SP 410 during roaming. Similarly, BSMs 423 and 413 have the same function as that of the BSM 104 of FIG. 1, BSDAs 422 and 412 have the same function as that of the BSDA 103 of FIG. 1, and group entities 421 and 411, each composed of BDS-SD, BDS and/or IN, have the same function as the group entity of the BDS-SD 111, the BDS 112 and/or the IN 113 of FIG. 1. A Terminal 400 has the same function as that of the Terminal 105 of FIG. 1. The above-mentioned entities are

not all used in the roaming procedure, so the entities used in the roaming procedure according to an exemplary embodiment of the present invention will be described.

[0072] In steps 401 and 402 corresponding to the part not directly specified in the roaming procedure, it is assumed that as the Terminal 400 arrives at the roaming area, the roaming procedure is automatically performed by the group entity 411 of BDS, IN and/or BDS-SD, and the BSDA 412, which are lower networks for transmitting the BCAST service. However, for reference, in step 401, the group entity 411 of BDS, IN and/or BDS-SD, which is a lower network of the BCAST, should perform roaming, provide the roaming indication information to the Terminal 400, and provide basic information based on which the Terminal 400 can receive the service guide. Using the basic information, the Terminal 400 can receive the service guide in step 402 by receiving the Service Guide Context fragment 201 of FIG. 2.

[0073] In step 402, upon receipt of the service guide, the Terminal 400 acquires the information described in Table 11.

[0074] In step 403, using the information acquired from Table 11, the Terminal 400 generates a message for making a roaming registration request to the Home SP 420, and sends the message to the BSM 423 of the Home SP 420. The contents of the Roaming Request message generated by the Terminal 400 in step 403 are shown in Table 12 below.

Table 12

Request ID
Terminal ID
Visited SP ID
Visited SP BSM ID
Visited BSDA ID
Purchase Item ID

[0075] Request ID, a first item of Table 12, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 4 until the time the roaming registration request procedure of FIG. 4 ends. Terminal ID is a unique ID for the terminal to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request. Visited SP ID is an identifier of the service provider that provides the service in the area where the roaming terminal stays. The Visited SP ID is used for providing the service provider of the Home SP 420 with the information indicating to whom the terminal make a roaming request. Here, when the BSM 423 of the Home SP 420 determines from the Visited SP ID that there is no roaming agreement made with the BSM 423 itself, the BSM 423 directly proceeds to step 406 where it can notify the roaming unavailability to the Terminal 400. Visited SP BSM ID is used for informing the Home SP of the entity that actually makes a negotiation on the roaming service registration procedure with the identifier of the BSM, used by the Visited SP 410. Visited BSDA ID is an identifier of the BSDA used by the Visited SP, and because one service provider can provide the service through several BSDAs, the Visited BSDA ID is used for indicating through which BSDA among the BSDAs used by the Visited SP the roaming terminal desires to receive the service. Finally, Purchase Item ID is used for indicating the service that the roaming user desires to receive. For the terminal that made the roaming registration request in step 403, the BSM 413 of the Visited SP 410 can additionally perform an authentication process on the terminal, and because the authentication process is not related to the basis of the present invention, a description thereof will be omitted for clarity and conciseness.

[0076] In step 404, for the roaming registration request received from the Terminal 400 in step 403, the BSM 423 of the Home SP 420 sends a roaming registration request to the BSM 413 of the Visited SP 410 to which the Terminal 400 is roaming. The contents of the message sent from the BSM 423 of the Home SP 420 to the BSM 413 of the Visited SP 410 in step 404 are shown in Table 13 below.

Table 13

Request ID
Terminal ID
Home SP ID
Home SP BSM ID
Visited BSDA ID
Terminal Subscription Type

(continued)

Purchase Item ID

5 **[0077]** Request ID, a first item of Table 13, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 4 until the time the roaming registration request procedure of FIG. 4 ends. Terminal ID is a unique ID for the terminal to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request. Home SP ID is used for indicating from which service provider the terminal that requested the roaming registration in the Visited SP 410 has originally received the service. Using this information, the BSM 413 of the Visited SP 410 can recognize that the roaming-requested terminal belongs to the service provider with whom its roaming agreement is made. Home SP BSM ID is used for informing the Visited SP 410 of the entity for a negotiation needed in the roaming registration process. The BSM 413 of the Visited SP 410 responds to the roaming registration result depending on the Home SP BSM ID. Visited BSDA ID is used for providing the Visited SP 410 with the information indicating in which service area the terminal is currently requesting the service. Terminal Subscription Type is information provided to the Visited SP 410 to evaluate in which class the roaming-requested terminal can receive services of the Visited SP 410, and it is evaluated along with Purchase Item ID. The Terminal Subscription Type can be a class of the service that the roaming-requested terminal can receive from the roaming-requested Visited SP 410 based on the roaming agreement made between the Home SP 420 and the Visited SP 410. This can be defined in the form of a roaming allowed class number or code agreed between the two service providers, and its form is not defined in an exemplary embodiment of the present invention. Purchase Item ID is a service requested by the terminal, and depending on whether it can be received with the separate cost or depending on a roaming agreement between the Visited SP 410 and the Home SP 420, its reception possibility is determined based on the evaluation on whether it is processed with subscription of the roaming-requested terminal.

25 **[0078]** In step 405, the BSM 413 of the Visited SP 410 sends a response to the request received in step 404. The main purpose in step 405 is to inform the available scope of the roaming service requested by the terminal using the information received in step 404. A scope of the service that the terminal can receive from the Visited SP 410 can also be provided along with authorization for the roaming service requested by the terminal. The message sent from the BSM 413 of the Visited SP 410 to the BSM 423 of the Home SP 420 in step 405 is shown in Table 14 below.

Table 14

Request ID
Roaming Authorization Status
Roaming Service Allowed Scope

[0079] Request ID, a first item of Table 14, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 4 until the time the roaming registration request procedure of FIG. 4 ends. Roaming Authorization Status is used for providing the evaluation result made on the roaming possibility using the information provided from the Visited SP 410 in step 404, to the BSM 423 of the Home SP 420 of the roaming-requested Terminal 400. Roaming Service Allowed Scope, when roaming is available, is used for allowing a value of the Terminal Subscription Type received in step 404 to indicate which reception right the roaming Terminal 400 will actually have in the Visited SP 410. The reception possibility of the service corresponding to the Purchase Item ID requested by the Terminal 400 is also defined in the Roaming Service Allowed Scope. In addition, the information related to occurrence of additional cost and a change in the charging system is also added to the Roaming Service Allowed Scope during roaming.

[0080] Steps 404 and 405 may also be omitted when necessary. For example, the steps can be omitted when the Terminal 400, after completing the roaming registration procedure, desires to make an additional service request while receiving the service. In this case, the BSM 423 of the Home SP 420 knows a part or all of the price policy for the roaming of the BSM 413 of the Visited SP 410.

[0081] In step 406, the Home SP 420 notifies the result on the roaming registration request received via the Visited SP 410 in step 405 to the Terminal 400. Actually, in step 406, the BSM 423 of the Home SP 420 forwards the message received in step 405, to the Terminal 400. After the Home SP 420 analyzes the roaming registration request of the terminal in step 403, if there is no roaming agreement with the Visited SP 410 in the area where the Terminal 400 stays, the Home SP 420 directly proceeds to step 406 where it fills the contents of Table 14 with a roaming request registration fail and sends it to the Terminal 400. In this case, the roaming is failed.

[0082] In step 407, the Terminal 400 sends a response to the roaming registration request that it sent to its Home SP 420. In this step, the Terminal 400 informs the BSM 413 of the Visited SP 410 whether it agrees with the Roaming Service Allowed Scope in the message received in step 406. If the Terminal 400 does not agree with the additional cost occurring during roaming or the change in the charging system, the roaming service is not achieved. However, if the Terminal 400 agrees, it proceeds to the next step. Table 15 below shows a message with which the Terminal 400 provides a final confirm for the roaming to the Visited SP 410.

Table 15

Request ID
Roaming Confirm Status

[0083] Request ID, a first item of Table 15, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 4 until the time the roaming registration request procedure of FIG. 4 ends. Roaming Confirm Status is an item used for informing the Visited SP 410 whether or not the Terminal 400 will perform the roaming.

[0084] In step 408, the Terminal 400 receives a Long-Term Key message used for deciphering the received service when it finally determined to receive the roaming service. The Terminal 400 receives the Long-Term Key message in step 408 using the long-term key reception method defined in the BCAST standard, and this method will not be dealt with in an exemplary embodiment of the present invention.

[0085] In step 409, the Terminal 400 receives the service from the Visited SP 410 through the roaming.

[0086] Although it is also possible to enable the roaming using the message items defined in FIG. 4 in the Service Provisioning message and procedure defined in OMA BCAST as well as the roaming procedure described in FIG. 4, this is not dealt with in the present invention. For the Service Provisioning, refer to the documents in the OMA web site [http://www.openmobilealliance.org/ftp/Public documents/BAC/ BCAST/ Permanent documents/OMA- TS- BCAST_Services-V1_0-20050909-D.zip](http://www.openmobilealliance.org/ftp/Public%20documents/BAC/BCAST/Permanent_documents/OMA-TS-BCAST_Services-V1_0-20050909-D.zip), which are incorporated by reference. The reference documents were the newest edition as of the filing date of this application, and if there is any update in the documents in the future, the updated edition will be applied.

[0087] FIG. 5 is a flowchart illustrating an operation of a BSM 413 of a Visited SP 410 according to an exemplary embodiment of the present invention. A description of FIG. 5 will be made with reference to FIG. 4.

[0088] In step 501, the BSM 413 of the Visited SP 410 receives a roaming registration request from a BSM 423 of a Home SP 420 of a roaming Terminal 400, and decipheres the received request message. The contents of the received message are shown in Table 13, and the BSM 413 of the Visited SP 410 analyzes Terminal Subscription Type among the contents of the received message in step 502. Thereafter, in step 503, the BSM 413 of the Visited SP 410 determines a roaming allowed scope by analyzing a relationship between subscription of the roaming-requested terminal and its subscription policy. If the subscription of the roaming-requested terminal is insufficient to support the roaming, the BSM 413 of the Visited SP 410 generates a message for rejecting the roaming request and delivers the generated message to the BSM 423 of the Home SP 420 in step 504. However, if it is determined that the roaming is available with subscription of the roaming-requested terminal, the BSM 413 of the Visited SP 410 determines in step 505 whether there is a particular requirement such as Purchase Item. If there is a particular requirement, the BSM 413 of the Visited SP 410 calculates the charge, and if there is no particular requirement, the BSM 413 of the Visited SP 410 calculates the additional charge occurring during the roaming. After completion of the calculation, the BSM 413 of the Visited SP 410 generates a response message to the roaming request. The contents of the generated message are shown in Table 14.

[0089] After completion of step 505, the BSM 413 of the Visited SP 410 waits for the final confirm for the roaming from the Terminal 400 in step 506. If the roaming-requested Terminal 410 sends a Final Confirm message for the roaming, the BSM 413 of the Visited SP 410 receives and decipheres the message in step 507. The contents of the received message are shown in Table 15, and the BSM 413 of the Visited SP 410 determines in step 508 whether the Terminal 400 agrees with the roaming condition. If the Terminal 400 does not agree with the roaming condition, the roaming procedure with the corresponding Terminal 400 is terminated. Otherwise, if the Terminal 400 agrees with the roaming condition, the BSM 413 of the Visited SP 410 sends a Long-Term Key message for deciphering the received service in step 509. Upon receipt of the Long-Term Key message, the Terminal 400 can use the roaming service within its agreed scope.

[0090] FIG. 6 is a flowchart illustrating an operation of a BSM 423 of a Home SP 420 according to an exemplary embodiment of the present invention. A description of FIG. 6 will be made with reference to FIG. 4.

[0091] In step 601, the BSM 423 of the Home SP 420 receives a Roaming Request message from a roaming Terminal 400, and decipheres the received message. The message received by the Home SP 420 is shown in Table 12. Using

the deciphered message, the BSM 423 of the Home SP 420 first determines in step 602 whether there is a roaming agreement with a Visited SP 410 where the roaming-requested Terminal 400 stays. If there is no agreement, the BSM 423 of the Home SP 420 proceeds to step 609 where it performs a no-roaming agreement process. In step 609, the BSM 423 of the Home SP 420 can also include the cause of the roaming unavailability, when necessary, while notifying Roaming Unavailable subscription, or can deliver the type of the partially available service if possible. However, if there is a roaming agreement, the BSM 423 of the Home SP 420 retrieves subscription of the corresponding Terminal 400 in step 603, and then determines in step 604 whether the retrieved subscription of the Terminal 400 is Roaming Allowable subscription.

[0092] If the retrieved subscription is Roaming Unsupported subscription, the BSM 423 of the Home SP 420 proceeds to step 609 to inform that the corresponding subscription is Roaming Unavailable subscription. In step 609, the BSM 423 of the Home SP 420 can include even the cause of the roaming unavailability when necessary while notifying the Roaming Unavailable subscription, or can deliver the type of the partially available service if possible. If the retrieved subscription is roaming-supported subscription, the BSM 423 of the Home SP 420 sends a Roaming Authorization Request message to a BSM 413 of the Visited SP 410 in step 605. The contents of this message are shown in Table 13. After sending the request message, the BSM 423 of the Home SP 420 waits for a response from the Visited SP 410 in step 606. Upon receipt of the response to the request, the BSM 423 of the Home SP 420 deciphers the received message in step 607, and analyzes the results on the requirement in step 608. If the requirement is permitted by the Visited SP 410, the BSM 423 of the Home SP 420 generates a message for notifying the results and delivers the message to the roaming-requested Terminal 400 in step 610. Otherwise, the BSM 423 of the Home SP 420 proceeds to step 609 where it can include even the cause of the roaming unavailability when necessary while notifying the Roaming Unavailable subscription, or can deliver the type of the partially available service if possible.

[0093] FIG. 7 is a flowchart illustrating an operation of a Terminal 400 according to an exemplary embodiment of the present invention. A description of FIG. 7 will be made with reference to FIG. 4.

[0094] The Terminal 400 can discover a Visited SP 410 through a lower BDS-SD 111, BDS 112 or IN 113 in an area other than the area of its Home SP 420, and detect the BCAST service of the corresponding area. Upon detecting the BCAST service, the Terminal 400 can find a Service Guide Context fragment 201 and fully receive the service guide using a Service Guide Delivery Descriptor fragment 202 depending on the Service Guide Context fragment 201 in step 701. Upon receipt of the service guide, the Terminal 400, if it desires to receive the roaming service, sends a Roaming Request message for roaming service authorization to a BSM 423 of its Home SP 420 in step 702. The contents of the sent message are shown in Table 12. After sending the Roaming Request message, the Terminal 400 waits for a response in step 703. If a roaming agreement between the BSM 423 of the Home SP 420 and the BSM 413 of the Visited SP 410 is determined, the Terminal 400 receives a response message to the request from the BSM 423 of the Home SP 420 and deciphers the received response message in step 704. The contents of the response message are shown in Table 14. Thereafter, the Terminal 400 determines in step 705 whether the roaming is available by deciphering the response message.

[0095] If the roaming is unavailable, the Terminal 400 gives up the roaming. However, if the roaming is available, the Terminal 400 checks the roaming condition in the Visited SP 410 in step 706 to determine whether the Terminal 400 is acceptable. If the Terminal 400 does not agree with the roaming condition, the Terminal 400 transmits a Confirm message for rejecting the roaming to the BSM 413 of the Visited SP 410 in step 707. However, if the Terminal 400 agrees with the roaming condition, the Terminal 400 sends a Confirm message indicating the agreement to the BSM 413 of the Visited SP 410 in step 708. After sending the agreement message, the Terminal 400 receives a Long-Term Key message in step 709, and receives the BCAST service after preparing for service or content deciphering in step 710.

[0096] A description will now be made of a roaming procedure according to an exemplary embodiment of the present invention.

[0097] FIG. 8 is a signaling diagram illustrating a roaming procedure according to an exemplary embodiment of the present invention.

[0098] Before a description of each step in the roaming procedure according to an exemplary embodiment of the present invention is given, each entity of FIG. 8 will be described.

[0099] BSAs 824 and 814 in a Home SP 820 and a Visited SP 810 are equal in function to the BSA 102 of FIG. 1, so they are separately shown to differentiate the BSA in the Home SP 820 from the BSA in the Visited SP 810 during roaming. Similarly, BSMs 823 and 813 have the same function as that of the BSM 104 of FIG. 1, BSDAs 822 and 812 have the same function as that of the BSDA 103 of FIG. 1, and group entities 821 and 811, each composed of BDS-SD, BDS and/or IN, have the same function as the group entity of the BDS-SD 111, the BDS 112 and/or the IN 113 of FIG. 1. A Terminal 800 has the same function as that of the Terminal 105 of FIG. 1. The above-mentioned entities are not all used in the roaming procedure according to an exemplary embodiment of the present invention, so the entities used in the roaming procedure will be described.

[0100] In steps 801 and 802 corresponding to the part not directly specified in the roaming procedure, it is assumed that as the Terminal 800 arrives at the roaming area, the roaming procedure is automatically performed by the group

entity 811 of BDS, IN and/or BDS-SD, and the BSDA 812, which are lower networks for supporting the BCAST service. However, for reference, in step 801, the group entity 811 of BDS, IN and/or BDS-SD, which is a lower network of the BCAST, should perform roaming, provide the roaming indication information to the Terminal 800, and provide basic information based on which the Terminal 800 can receive the service guide. Using the basic information, the Terminal 800 can receive the service guide in step 802 by receiving the Service Guide Context fragment 201 of FIG. 2.

[0101] In step 802, upon receipt of the service guide, the Terminal 800 acquires the information described in Table 11.

[0102] In step 803, using the information acquired from Table 11, the Terminal 800 generates a Roaming Request message for making a roaming registration request to the Visited SP 810, and sends the message to the BSM 813 of the Visited SP 810. The contents of the Roaming Request message generated by the Terminal 800 in step 803 are shown in Table 16 below.

Table 16

Request ID
Terminal ID
Home SP ID
Home SP BSM ID
Purchase Item ID

[0103] Request ID, a first item of Table 16, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 8 until the time the roaming registration request procedure of FIG. 8 ends. Terminal ID is a unique ID for the terminal to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request. Home SP ID is an identifier used for allowing the roaming terminal to inform the Visited SP 810 who its Home SP 820 is. Using this information, the Visited SP 810 can determine to which entity the roaming-requested Terminal 800 originally belongs, and can also determine a roaming relationship with the corresponding entity. Here, when the BSM 813 of the Visited SP 810 determines from the Home SP ID that there is no roaming agreement made with the BSM 813 itself, the BSM 813 directly proceeds to step 806 where it can notify a roaming unavailability to the Terminal 800.

[0104] Home SP BSM ID is used for informing the Visited SP 810 of the entity that actually makes a negotiation on the roaming service registration procedure with the identifier of the BSM, used by the Home SP 820. Finally, Purchase Item ID is used for indicating the service that the roaming user desires to receive. For the terminal that made the roaming registration request in step 803, the BSM 813 of the Visited SP 810 can additionally perform an authentication process on the terminal. This can be performed spontaneously by the BSM 813 of the Visited SP 810, or can be performed through a connection with a BSM 823 of the Home SP 820 or through the third authentication entity. Because the authentication process is not related to the basis of the present invention, a description thereof will be omitted herein for clarity and conciseness.

[0105] In step 804, for the roaming registration request received from the Terminal 800 in step 803, the BSM 813 of the Visited SP 810 sends a roaming registration request to the BSM 823 of the Home SP 820 of the Terminal 800. The contents of the message sent from the BSM 813 of the Visited SP 810 to the BSM 823 of the Home SP 820 in step 804 are shown in Table 17 below.

Table 17

Request ID
Terminal ID
Visited SP ID
Visited SP BSM ID

[0106] Request ID, a first item of Table 17, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 8 until the time the roaming registration request procedure of FIG. 8 ends. Terminal ID is a unique ID for the terminal to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request. Visited SP ID is used by the Visited SP 810 to provide its own information to the BSM 823 of the Home SP 820 of the roaming-requested terminal.

Visited SP BSM ID is used for providing the BSM 823 of the Home SP 820 with the information indicating the entity with which the Visited SP 810 will make a roaming-related negotiation. This is because the Visited SP 810 can have several BSMs.

5 **[0107]** In step 805, the BSM 823 of the Home SP 820 sends a response to the roaming registration request received in step 804. Table 18 below shows the contents of the message sent from the BSM 823 of the Home SP 820 to the BSM 813 of the Visited SP 810.

Table 18

Request ID
Roaming Authorization Status
Terminal Subscription Type

15 **[0108]** Request ID, a first item of Table 18, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 8 until the time the roaming registration request procedure of FIG. 8 ends. Roaming Authorization Status is used for allowing the Home SP 820 to determine whether the roaming is authorized by retrieving subscription of the roaming-requested Terminal 800 in the Visited SP 810 using the Terminal ID received in step 804, and to provide the results to the Visited SP 810. Terminal Subscription Type is information provided so that the Visited SP 810 can evaluate which reception right the roaming Terminal 800 will have in the Visited SP 810. The Terminal Subscription Type can be a class of the service that the roaming-requested Terminal 800 can receive from the roaming-requested Visited SP 810 based on the roaming agreement made between the Home SP 820 and the Visited SP 810. This can be defined in the form of a roaming allowed class number or code agreed between the two service providers, and its form is not defined in an exemplary embodiment of the present invention.

25 **[0109]** Steps 804 and 805 may also be omitted when necessary. For example, the steps can be omitted when the Terminal 800, after completing the roaming registration procedure, desires to make an additional service request while receiving the service.

30 **[0110]** In step 806, the Visited SP 810 sends a response to the received roaming registration request to the Terminal 800. The contents of the message sent from the BSM 813 of the Visited SP 810 to the Terminal 800 in step 806 are shown in Table 19 below.

Table 19

Request ID
Roaming Authorization Status
Roaming Service Allowed Scope

35 **[0111]** Request ID, a first item of Table 19, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 8 until the time the roaming registration request procedure of FIG. 8 ends. Roaming Authorization Status is used for providing the evaluation result made on the roaming possibility using the information provided from the Home SP 820 in step 805, to the roaming-requested Terminal 800.

40 **[0112]** Roaming Service Allowed Scope, when roaming is available, is used for allowing a value of the Terminal Subscription Type received in step 805 to indicate which reception right the roaming Terminal 800 will actually have in the Visited SP 810. The reception possibility of the service corresponding to the Purchase Item ID requested by the Terminal 800 is also defined in the Roaming Service Allowed Scope. In addition, the information related to occurrence of additional cost and a change in the charging system is also added to the Roaming Service Allowed Scope during roaming.

45 **[0113]** In step 807, the Terminal 800 informs the BSM 813 of the Visited SP 810 whether it agrees with the information in the Roaming Service Allowed Scope in the message received in step 806 as a response to the roaming registration request to its Visited SP 810. If the Terminal 800 does not agree with the additional cost occurring during roaming or the change in the charging system, the roaming service is not achieved. However, if the Terminal 800 agrees, it proceeds to the next step. Table 20 below shows a Confirm message with which the Terminal 800 provides a final confirm for the roaming to the Visited SP 810.

Table 20

Request ID
Roaming Confirm Status

5

10

15

20

25

30

35

40

45

50

55

[0114] Request ID, a first item of Table 20, is an identifier given for enabling to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 8 until the time the roaming registration request procedure of FIG. 8 ends. Roaming Confirm Status is an item used for indicating whether or not the Terminal 800 will roam to the Visited SP 810.

[0115] In step 808, the Terminal 800 receives a Long-Term Key message used for deciphering the received service when it finally determined to receive the roaming service. The Terminal 800 receives the Long-Term Key message in step 808 using the long-term key reception method defined in the BCAST standard, which this method will not be dealt with in an exemplary embodiment of the present invention.

[0116] In step 809, the Terminal 800 receives the service from the Visited SP 810 through the roaming.

[0117] Although it is also possible to enable the roaming using the message items defined in FIG. 8 in the Service Provisioning message and procedure defined in OMA BCAST as well as the roaming procedure described in FIG. 8, this is not dealt with in an exemplary embodiment of the present invention. For the Service Provisioning, refer to the documents in the OMA web site http://www.openmobilealliance.org/ftp/Public_documents/BAC/BCAST/Permanent_documents/OMA-TS-BCAST_Services-V1_0-20050909-D.zip, which are incorporated by reference. The reference documents were the newest edition as of the filing date of this application, and if there is any update in the documents in the future, the updated edition will be applied.

[0118] FIG. 9 is a flowchart illustrating an operation of a BSM 813 of a Visited SP 810 according to an exemplary embodiment of the present invention. A description of FIG. 9 will be made with reference to FIG. 8.

[0119] In step 901, the BSM 813 of the Visited SP 810 receives a Roaming Request message for a roaming registration request from a roaming Terminal 800, and decipheres the received message. The contents of the received message are shown in Table 16. Using the deciphered contents of the message, the BSM 813 of the Visited SP 810 determines in step 902 whether the roaming-requested Terminal 800 is a terminal of the service provider having a roaming agreement with the Terminal 800 itself. If the roaming-requested Terminal 800 is a terminal belonging to the service provider having no roaming agreement with the Terminal 800 itself, the BSM 813 of the Visited SP 810 proceeds to step 907 where it transmits a Roaming Unavailable Response message (or Roaming Service Unauthorized Response message) to the Terminal 800. In step 907, the BSM 813 of the Visited SP 810 can include even the cause of the roaming unavailability when necessary while transmitting the Roaming Unavailable message, or can deliver the type of the partially available service if possible.

[0120] However, if the Terminal 800 belongs to the service provider having a roaming agreement with the Terminal 800 itself, the BSM 813 of the Visited SP 810 transmits a Terminal Request message to the BSM 823 of the Home SP 820 of the roaming-requested terminal in step 903. The contents of the transmitted message are shown in Table 17. Thereafter, in step 904, the BSM 813 of the Visited SP 810 waits for a response message from the BSM 823 of the Home SP 820 of the roaming-requested Terminal 800. Upon receipt of the response message from the BSM 823 of the Home SP 820, the BSM 813 of the Visited SP 810 decipheres the received message in step 905. The contents of the received message are shown in Table 18. Thereafter, in step 906, the BSM 813 of the Visited SP 810 checks the contents of the received message, and then determines whether it can authorize the Terminal 800 to perform the roaming and whether it will authorize the Terminal 800 to perform the roaming using the subscription information of the terminal. If the BSM 813 of the Visited SP 810 cannot authorize the Terminal 800 to perform the roaming, it transmits a Roaming Unavailable message to the terminal in step 907. In step 907, the BSM 813 of the Visited SP 810 can include even the cause of the roaming unavailability when necessary while transmitting the Roaming Unavailable message, or can deliver the type of the partially available service if possible.

[0121] If the BSM 813 of the Visited SP 810 can authorize the Terminal 800 to perform the roaming, it generates a response message taking into account the additional charge occurring during roaming and the change in the charging system using the subscription information of the Terminal 800, and transmits the response message to the terminal in step 908. After transmitting the response message, the BSM 813 of the Visited SP 810 waits for a response from the Terminal 800 in step 909. Upon receipt of the Final Confirm message for the roaming from the Terminal 800, the BSM 813 of the Visited SP 810 decipheres the received message in step 910, and determines in step 911 whether the terminal has roamed. If the contents of the received message indicate roaming rejection, the roaming request procedure is terminated. Otherwise, if the contents of the received message indicate roaming acceptance, a Long-Term Key message is transmitted to the terminal in step 912.

[0122] FIG. 10 is a flowchart illustrating an operation of a BSM 823 of a Home SP 820 according to an exemplary embodiment of the present invention. A description of FIG. 10 will be made with reference to FIG. 8.

[0123] In step 1001, the BSM 823 of the Home SP 820 receives a Roaming Request message for a roaming-requested terminal from a BSM 813 of a Visited SP 810. The contents of the message received by the Home SP 820 are shown in Table 17. The BSM 823 of the Home SP 820 retrieves subscription of the roaming-requested terminal in the Visited SP 810 in step 1002, and determines in step 1003 whether the roaming-requested Terminal 800 is allowed to receive the roaming service. If the roaming-requested Terminal 800 is allowed to receive the roaming service, the BSM 823 of the Home SP 820 transmits in step 1005 to the Visited SP 810 a message including the contents shown in Table 18 where the subscription of the Terminal 800 is included. If the roaming-requested Terminal 800 is not authorized to receive the roaming service, the BSM 823 of the Home SP 820 transmits a Roaming Unavailable message (or Roaming Unauthorized message) to the Visited SP 810 in step 1004. Here, the contents of the message are shown in Table 14.

[0124] FIG. 11 is a flowchart illustrating an operation of a Terminal 800 according to an exemplary embodiment of the present invention. A description of FIG. 11 will be made with reference to FIG. 8.

[0125] The Terminal 800 can discover a Visited SP 810 through a lower BDS-SD 111, BDS 112 or IN 113 in an area other than the area of its Home SP 820, and detect the BCAST service of the corresponding area. Upon detecting the BCAST service, the Terminal 800 can find a Service Guide Context fragment 201 and fully receive the service guide using a Service Guide Delivery Descriptor fragment 202 depending on the Service Guide Context fragment 201 in step 1101. Upon receipt of the service guide, the Terminal 800, if it desires to receive the roaming service, sends a Roaming Request message for roaming service authorization to a BSM 813 of the Visited SP 810 in step 1102. The contents of the sent message are shown in Table 16.

[0126] After sending the Roaming Request message, the Terminal 800 waits for a response in step 1103. If a roaming agreement between the BSM 823 of the Home SP 820 and the BSM 813 of the Visited SP 810 is determined, the Terminal 800 receives a response message to the request from the BSM 813 of the Visited SP 810 and deciphers the received response message in step 1104. The contents of the response message are shown in Table 19. Thereafter, the Terminal 800 determines in step 1105 whether the roaming is available by deciphering the response message.

[0127] If the roaming is unavailable, the Terminal 800 gives up the roaming. However, if the roaming is available, the Terminal 800 checks the roaming condition in the Visited SP 810 in step 1106 to determine whether the Terminal 800 is acceptable. If the Terminal 800 does not agree with the roaming condition, the Terminal 800 transmits a Confirm message for rejecting the roaming to the BSM 813 of the Visited SP 810 in step 1107. However, if the Terminal 800 agrees with the roaming condition, the Terminal 800 sends a Confirm message indicating the agreement to the BSM 813 of the Visited SP 810 in step 1108. After sending the agreement message, the Terminal 800 receives a Long-Term Key message in step 1109, and receives the BCAST service after preparing for service or content deciphering in step 1110.

[0128] FIG. 13 is a signaling diagram illustrating a roaming procedure according to an exemplary embodiment of the present invention. Before a description of each step in the roaming procedure according to the third embodiment is given, each entity of FIG. 13 will be described. BSAs 1324 and 1314 in a Home SP 1320 and a Visited SP 1310 are equal in function to the BSA 102 of FIG. 1, so they are separately shown to differentiate the BSA in the Home SP 1320 from the BSA in the Visited SP 1310 during roaming. Similarly, BSMs 1323 and 1313 have the same function as that of the BSM 104 of FIG. 1, BSDAs 1322 and 1312 have the same function as that of the BSDA 103 of FIG. 1, and group entities 1321 and 1311, each composed of BDS-SD, BDS and/or IN, have the same function as the group entity of the BDS-SD 111, the BDS 112 and/or the IN 113 of FIG. 1. A Terminal 1300 has the same function as that of the Terminal 105 of FIG. 1. The above-mentioned entities are not all used in the roaming procedure according to an exemplary embodiment of the present invention, so the entities used in the roaming procedure will be described.

[0129] As shown in FIG. 13, in steps 1301 and 1302 corresponding to the part not directly specified in the roaming procedure, it is assumed that as the Terminal 1300 arrives at the roaming area, the roaming procedure is automatically performed by the group entity 1311 of BDS, IN and/or BDS-SD, and the BSDA 1312, which are lower networks for supporting the BCAST service. However, for reference, in step 1301, the group entity 1311 of BDS, IN and/or BDS-SD, which is a lower network of the BCAST, should perform roaming, provide the roaming indication information to the Terminal 1300, and provide basic information based on which the Terminal 1300 can receive the service guide. Using the basic information, the Terminal 1300 can receive the service guide in step 1302 by receiving the Service Guide Context fragment 201 of FIG. 2.

[0130] In step 1302, upon receipt of the service guide, the Terminal 1300 acquires the information described in Table 11. In step 1303, the Terminal 1300 generates a Roaming Request message for making a roaming registration request to the Home SP 1320 using the information acquired from Table 11, and sends the Roaming Request message to the BSM 1323 of the Home SP 1320. The contents of the Roaming Request message generated by the Terminal 1300 in step 1303 are shown in Table 21.

Table 21

Request ID
Terminal ID
Visited SP ID
Visited SP BSM ID
Visited BSDA ID
Purchase Item ID

[0131] Request ID, a first item of Table 21, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 13 until the time the roaming registration request procedure of FIG. 13 ends. Terminal ID is a unique ID for the terminal for enabling to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request.

[0132] Visited SP ID is an identifier of the service provider that provides the service in the area where the roaming terminal stays. The Visited SP ID is used for providing the service provider of the Home SP 1320 with the information indicating to whom the terminal make a roaming request. Here, when the BSM 1323 of the Home SP 1320 determines from the Visited SP ID that there is no roaming agreement made with the BSM 1323 itself, the BSM 1323 directly proceeds to step 1306 where it can notify a roaming unavailability to the Terminal 1300. Visited SP BSM ID is used for informing the Home SP 1320 of the entity that actually makes a negotiation on the roaming service registration procedure with the identifier of the BSM, used by the Visited SP 1310. Visited BSDA ID is an identifier of the BSDA used by the Visited SP 1310, and because one service provider can provide the service through several BSDAs, the Visited BSDA ID is used for indicating through which BSDA the roaming Terminal 1300 desires to receive the service. Finally, Purchase Item ID is used for indicating the service that the roaming user desires to receive. For the Terminal 1300 that made the roaming registration request in step 1303, the BSM 1323 of the Home SP 1320 can additionally perform an authentication process on the Terminal 1300, and the detailed authentication process will not be dealt with in an exemplary embodiment of the present invention.

[0133] In step 1304, for the roaming registration request received from the Terminal 1300 in step 1303, the Terminal 1300 sends a roaming registration request to the BSM 1313 of its roaming Visited SP 1310. The contents of the message sent from the BSM 1323 of the Home SP 1320 to the BSM 1313 of the Visited SP 1310 in step 1304 are shown in Table 22.

Table 22

Request ID
Terminal ID
Home SP ID
Home SP BSM ID
Visited BSDA ID
Terminal Subscription Type
Purchase Item ID

[0134] Request ID, a first item of Table 22, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 13 until the time the roaming registration request procedure of FIG. 13 ends. Terminal ID is a unique ID for the terminal for enabling to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request. Home SP ID is used for indicating from which service provider the terminal that requested the roaming registration in the Visited SP 1310 has originally received the service. Using this information, the BSM 1313 of the Visited SP 1310 can recognize that the roaming-requested Terminal 1300 belongs to the service provider with whom its roaming agreement is made. Home SP BSM ID is used for informing the Visited SP 1310 of the entity for a negotiation needed in the roaming registration process. The BSM 1313 of the Visited SP 1310 responds to the roaming registration result depending on the Home SP BSM ID. Visited BSDA ID is used for providing the Visited SP 1310 with the information indicating in which service area the terminal is currently requesting the service. Terminal Subscription Type is information provided to the

Visited SP 1310 to evaluate in which class the roaming-requested Terminal 1300 can receive services of the Visited SP 1310, and it is evaluated along with Purchase Item ID. The Terminal Subscription Type can be a class of the service that the roaming-requested Terminal 1300 can receive from the roaming-requested Visited SP 1310 based on the roaming agreement made between the Home SP 1320 and the Visited SP 1310. This can be defined in the form of a

5 roaming allowed class number or code agreed between the two service providers, and its form is not defined in this invention. Purchase Item ID is a service requested by the terminal, and depending on whether it can be received with the separate cost or depending on a roaming agreement between the Visited SP 1310 and the Home SP 1320, its reception possibility is determined based on the evaluation on whether it is processed with subscription of the roaming-requested terminal.

10 **[0135]** In step 1305, the BSM 1313 of the Visited SP 1310 sends a response to the request received in step 1304. The main purpose in step 1305 is to inform the available scope of the roaming service requested by the terminal using the information received in step 1304. A scope of the service that the terminal can receive from the Visited SP 1310 can also be provided along with authorization for the roaming service requested by the terminal. The message sent from the BSM 1313 of the Visited SP 1310 to the BSM 1323 of the Home SP 1320 in step 1305 is shown in Table 23 below.

Table 23

Request ID
Roaming Authorization Status
Roaming Service Allowed Scope

[0136] Request ID, a first item of Table 23, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID is constant from the time it is generated in FIG. 13 until the time the roaming registration request procedure of FIG. 13 ends. Roaming Authorization Status is used for providing the evaluation result made on the roaming possibility using the information provided from the Visited SP 1310 in step 1304, to the BSM 1323 of the Home SP 1320 of the roaming-requested Terminal 1300. Roaming Service Allowed Scope, when roaming is available, is used for allowing a value of the Terminal Subscription Type received in step 1304 to indicate which reception right the roaming Terminal 1300 will actually have in the Visited SP 1310. The reception possibility of the service corresponding to the Purchase Item ID requested by the Terminal 1300 is also defined in the Roaming Service Allowed Scope. In addition, the information related to occurrence of additional cost and a change in the charging system is also added to the Roaming Service Allowed Scope during roaming.

[0137] Steps 1304 and 1305 may also be omitted when necessary. For example, the steps can be omitted when the Terminal 1300, after completing the roaming registration procedure, desires to make an additional service request while receiving the service. In this case, the BSM 1323 of the Home SP 1320 knows a part or all of the price policy for the roaming of the BSM 1313 of the Visited SP 1310.

[0138] In step 1306, the Home SP 1320 notifies the result on the roaming registration request received via the Visited SP 1310 in step 1305 to the Terminal 1300. Actually, in step 1306, the BSM 1323 of the Home SP 1320 forwards the message received in step 1305, to the Terminal 1300. After the Home SP 1320 analyzes the roaming registration request of the terminal in step 1303, if there is no roaming agreement with the Visited SP 1310 in the area where the Terminal 1300 stays, the Home SP 1320 directly proceeds to step 1306 where it fills the contents of Table 23 with a roaming request registration fail and sends it to the Terminal 1300. In this case, the roaming is failed.

[0139] In step 1307, the Terminal 1300 sends a response to the roaming registration request that it sent to its Home SP 1320. In this step, the Terminal 1300 informs the BSM 1323 of the Visited SP 1320 whether it agrees with information in the Roaming Service Allowed Scope in the message received in step 1306. If the Terminal 1300 does not agree with the additional cost occurring during roaming or the change in the charging system, the roaming service is not achieved. However, if the Terminal 1300 agrees, it proceeds to the next step. Table 24 below shows a message with which the Terminal 1300 provides a final confirm for the roaming to the Home SP 1320.

Table 24

Request ID
Roaming Confirm Status

[0140] Request ID, a first item of Table 24, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its

own roaming registration request. The Request ID is constant from the time it is generated in FIG. 13 until the time the roaming registration request procedure of FIG. 13 ends. Roaming Confirm Status is an item used for informing the Home SP 1320 whether or not the Terminal 1300 will perform the roaming.

5 [0141] In step 1308, as the Terminal 1300 agrees with the roaming in step 1307, the BSM 1323 of the Home SP 1320 sends to the BSM 1313 of the Visited SP 1310 a Long-Term Key message necessary for deciphering the service requested by the Terminal 1300.

[0142] In step 1309, the BSM 1313 of the Visited SP 1310 delivers the Long-Term Key message requested by the BSM 1323 of the Home SP 1320.

10 [0143] In step 1325, the BSM 1323 of the Home SP 1320 delivers the Long-Term Key message necessary for deciphering the roaming service requested by the Terminal 1300.

[0144] Steps 1308, 1309 and 1325 are achieved using the long-term key transmission/reception method defined in the BCAST standard, and a detailed process thereof will now be dealt with in an exemplary embodiment of the present invention.

[0145] In step 1326, the Terminal 1300 receives the service of the Visited SP 1310 through the roaming.

15 [0146] Although it is also possible to enable the roaming using the message items defined in FIG. 13 in the Service Provisioning message and procedure defined in OMA BCAST as well as the roaming procedure described in FIG. 13, this is not dealt with in the present invention. For the Service Provisioning, refer to the documents in the OMA web site http://www.openmobilealliance.org/ftp/Public_documents/BAC/BCAST/Permanent_documents/OMA-TS-BCAST_Services-V1_0-20050909-D.zip, which are incorporated by reference. The reference documents were the newest edition as of the filing date of this application, and if there is any update in the documents in the future, the updated edition will be applied.

[0147] FIG. 14 is a flowchart illustrating an operation of a BSM 1313 of a Visited SP 1310 according to an exemplary embodiment of the present invention. A description of FIG. 14 will be made with reference to FIG. 13.

25 [0148] In step 1401, the BSM 1313 of the Visited SP 1310 receives a roaming registration request from a BSM 1323 of a Home SP 1320 of a roaming Terminal 1300, and decipheres the received request message. The contents of the received message are shown in Table 22, and the BSM 1313 of the Visited SP 1310 analyzes Terminal Subscription Type among the contents of the received message in step 1402. Thereafter, in step 1403, the BSM 1313 of the Visited SP 1310 determines a roaming allowed scope by analyzing a relationship between subscription of the roaming-requested terminal and its subscription policy. If the subscription of the roaming-requested terminal is insufficient to support the roaming, the BSM 1323 of the Home SP 1320 generates a message for rejecting the roaming request and delivers the generated message to the BSM 1323 of the Home SP 1320 in step 1404. However, if it is determined that the roaming is available with subscription of the roaming-requested Terminal 1300, the BSM 1313 of the Visited SP 1310 determines in step 1405 whether there is a particular requirement such as Purchase Item. If there is a particular requirement, the BSM 1313 of the Visited SP 1310 calculates the charge, and if there is no particular requirement, the BSM 1313 of the Visited SP 1310 calculates the additional charge occurring during the roaming. After completion of the calculation, the BSM 1313 of the Visited SP 1310 generates a response message to the roaming request. The contents of the generated message are shown in Table 23.

35 [0149] After completion of step 1405, the BSM 1313 of the Visited SP 1310 waits for the final confirm for the roaming from the Home SP 1320 in step 1406. Upon receipt of a Final Confirm message for the roaming of the roaming-requested Terminal 1300 from the Home SP 1320, the BSM 1313 of the Visited SP 1310 decipheres the received message in step 1407. After deciphering the received message, the BSM 1313 of the Visited SP 1310 determines in step 1408 whether the Terminal 1300 agrees with the roaming condition. If the Terminal 1300 does not agree with the roaming condition, the corresponding roaming procedure is terminated. Otherwise, if the Terminal 1300 agrees with the roaming condition, the BSM 1313 of the Visited SP 1310 sends a Long-Term Key message for deciphering the received service to the Home SP 1320 in step 1409. Upon receipt of the Long-Term Key message, the Home SP 1320 forwards the received Long-Term Key message to the Terminal 1300 so that the Terminal 1300 may use the roaming service within its agreed scope.

40 [0150] FIGs. 15A and 15B are flowcharts illustrating an operation of a BSM 1323 of a Home SP 1320 according to an exemplary embodiment of the present invention. A description of FIGs. 15A and 15B will be made with reference to FIG. 13.

50 [0151] In step 1501, the BSM 1323 of the Home SP 1320 receives a Roaming Request message for a roaming registration request from a roaming Terminal 1300, and decipheres the received message. The message received by the Home SP 1320 is shown in Table 21. Using the deciphered message, the BSM 1323 of the Home SP 1320 first determines in step 1502 whether there is a roaming agreement with a Visited SP 1310 where the roaming-requested Terminal 1300 stays. If there is no agreement, the BSM 1323 of the Home SP 1320 proceeds to step 1509 where it performs a no-roaming agreement process. In step 1509, the BSM 1323 of the Home SP 1320 can include even the cause of the roaming unavailability when necessary while notifying Roaming Unavailable subscription, or can deliver the type of the partially available service if possible. However, if there is a roaming agreement, the BSM 1323 of the Home SP 1320 retrieves subscription of the corresponding Terminal 1300 in step 1503, and then determines in step 1504 whether the

retrieved subscription of the Terminal 1300 is a Roaming Allowable subscription.

[0152] If the retrieved subscription is a Roaming Unsupported subscription, the BSM 1323 of the Home SP 1320 proceeds to step 1509 to inform that the corresponding subscription is a Roaming Unavailable subscription. In step 1509, the BSM 1323 of the Home SP 1320 can also include the cause of the roaming unavailability when necessary while notifying the Roaming Unavailable subscription, or can deliver the type of the partially available service if possible. If the retrieved subscription is Roaming Supported subscription, the BSM 1323 of the Home SP 1320 sends a Roaming Authorization Request message to a BSM 1313 of the Visited SP 1310 in step 1505. The contents of this message are shown in Table 22. After sending the request message, the BSM 1323 of the Home SP 1320 waits for a response from the Visited SP 1310 in step 1506. Upon receipt of the response to the request, the BSM 1323 of the Home SP 1320 deciphers the received message in step 1507, and analyzes the results on the requirement in step 1508. If the requirement is unacceptable, the BSM 1323 of the Home SP 1320 proceeds to step 1509 where it can also include the cause of the roaming unavailability when necessary while notifying the Roaming Unavailable subscription, or can deliver the type of the partially available service if possible. However, if it is determined that roaming is available with subscription of the roaming-requested terminal, the BSM 1323 of the Home SP 1320 determines in step 1510 whether there is a particular requirement such as Purchase Item, in addition to the message received in step 1507. If there is a particular requirement, the BSM 1323 of the Home SP 1320 calculates the charge, and if there is no particular requirement, the BSM 1323 of the Home SP 1320 calculates the additional charge occurring during the roaming. After completion of the calculation, the BSM 1323 of the Home SP 1320 generates a response message to the roaming request. The contents of the generated message are shown in Table 23.

[0153] After completion of step 1510, the BSM 1323 of the Home SP 1320 waits for the final confirm for the roaming from the Terminal 1300 in step 1511. Upon receipt of a Final Confirm message for the roaming from the Terminal 1300, the BSM 1323 of the Home SP 1320 deciphers the received message in step 1512. The contents of the received message are shown in Table 24, and the BSM 1323 of the Home SP 1320 determines in step 1513 whether the Terminal 1300 agrees with the roaming condition. If the Terminal 1300 does not agree with the roaming condition, the corresponding roaming procedure is terminated. Otherwise, if the Terminal 1300 agrees with the roaming condition, the BSM 1323 of the Home SP 1320 sends a request for a Long-Term Key message for deciphering the received service and waits for the Long-Term Key message in step 1514. Upon receipt of the Long-Term Key message from the Visited SP 1310 in step 1515, the Home SP 1320 forwards the received Long-Term Key message to the Terminal 1300 in step 1516, so the Terminal 1300 can use the roaming service within its agreed scope.

[0154] FIG. 16 is a flowchart illustrating an operation of a Terminal 1300 according to an exemplary embodiment of the present invention. A description of FIG. 16 will be made with reference to FIG. 13.

[0155] The Terminal 1300 can discover a Visited SP 1310 through a lower BDS-SD 111, BDS 112 or IN 113 in an area other than the area of its Home SP 1320, and detect the BCAST service of the corresponding area. Upon detecting the BCAST service, the Terminal 1300 can find a Service Guide Context fragment 201 and fully receive the service guide using a Service Guide Delivery Descriptor fragment 202 depending on the Service Guide Context fragment 201 in step 1601. Upon receipt of the service guide, the Terminal 1300, if it desires to receive the roaming service, sends a Roaming Request message for roaming service authorization to a BSM 1323 of its Home SP 1320 in step 1602. The contents of the sent message are shown in Table 21. After sending the Roaming Request message, the Terminal 1300 waits for a response in step 1603. If a roaming agreement between the BSM 1323 of the Home SP 1320 and the BSM 1313 of the Visited SP 1310 is determined, the Terminal 1300 receives a response message to the request from the BSM 1323 of the Home SP 1320 and deciphers the received response message in step 1604. The contents of the response message are shown in Table 23. Thereafter, the Terminal 1300 determines in step 1605 whether the roaming is available by deciphering the response message.

[0156] If the roaming is unavailable, the Terminal 1300 gives up the roaming. However, if the roaming is available, the Terminal 1300 checks the roaming condition in the Visited SP 1310 in step 1606 to determine whether the Terminal 1300 is acceptable. If the Terminal 1300 does not agree with the roaming condition, the Terminal 1300 transmits a Confirm message for rejecting the roaming to the BSM 1323 of the Home SP 1320 in step 1607. However, if the Terminal 1300 agrees with the roaming condition, the Terminal 1300 sends a Confirm message indicating the agreement to the BSM 1323 of the Home SP 1320 in step 1608. After sending the agreement message, the Terminal 1300 receives a Long-Term Key message in step 1609, and receives the BCAST service after preparing for service or content deciphering in step 1610.

[0157] A description will now be made of a purchase item list request procedure for roaming according to a fourth embodiment of the present invention.

[0158] FIG. 17 is a signaling diagram illustrating a purchase item list request procedure for roaming according to an exemplary embodiment of the present invention. Before a description of each step in the purchase item list request procedure for roaming according to an exemplary embodiment is given, each entity of FIG. 17 will first be described.

[0159] BSAs 1724 and 1714 in a Home SP 1720 and a Visited SP 1710 are equal in function to the BSA 102 of FIG. 1, so they are separately shown to differentiate the BSA in the Home SP 1720 from the BSA in the Visited SP 1710

during roaming. Similarly, BSMs 1723 and 1713 have the same function as that of the BSM 104 of FIG. 1, BSDAs 1722 and 1712 have the same function as that of the BSDA 103 of FIG. 1, and group entities 1721 and 1711, each composed of BDS-SD, BDS and/or IN, have the same function as the group entity of the BDS-SD 111, the BDS 112 and/or the IN 113 of FIG. 1. A Terminal 1700 has the same function as that of the Terminal 105 of FIG. 1. The above-mentioned entities are not all used in the purchase item list request procedure for roaming according to an exemplary embodiment of the present invention, so the entities used in the purchase item list request procedure for roaming will be described. The procedure shown in FIG. 17 can be optionally used during roaming, and it can be used between steps 402 and 403 of FIG. 4, or between steps 1302 and 1303 of FIG. 13.

[0160] Referring to FIG. 17, in step 1701, using the information shown in Table 11 acquired through reception of a service guide, the Terminal 1700 generates a Purchase Item List Request message for requesting information indicating which purchase items the Terminal 1700 can join during the roaming, and sends the generated message to the BSM 1723 of the Home SP 1720. The contents of the Purchase Item List Request message generated by the Terminal 1700 in step 1701 are shown in Table 25 below.

Table 25

Request ID
Terminal ID
Visited SP ID
Visited SP BSM ID
Visited BSDA ID

[0161] Request ID, a first item of Table 25, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID can be used together with the purchase item list request procedure for roaming shown in FIG. 17, and is equal to the Request ID in Tables 16-20 or Tables 21-24. Terminal ID is a unique ID for the terminal for enabling to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request. Visited SP ID is an identifier of the service provider that provides the service in the area where the roaming terminal stays.

[0162] The Visited SP ID is used for providing the service provider of the Home SP 1720 with the information indicating to whom the terminal make a roaming request. Here, when the BSM 1723 of the Home SP 1720 determines from the Visited SP ID that there is no roaming agreement made with the BSM 1723 itself, the BSM 1723 directly proceeds to step 1704 where it can notify the roaming unavailability to the Terminal 1700. Visited SP BSM ID is used for informing the Home SP of the entity that actually makes a negotiation on the roaming service registration procedure with the identifier of the BSM, used by the Visited SP 1710.

[0163] Visited BSDA ID is an identifier of the BSDA used by the Visited SP 1710, and because one service provider can provide the service through several BSDAs, the Visited BSDA ID is used for indicating through which BSDA among the BSDAs used by the Visited SP 1710 the roaming Terminal 1700 desires to receive the service. For the terminal that made the purchase item list request for roaming in step 1701, the BSM 1723 of the Home SP 1720 can additionally perform an authentication process on the terminal, and because the authentication process is not related to the basis of the present invention, a description thereof will be omitted herein for clarity and conciseness.

[0164] In step 1702, upon receipt of the Purchase Item List Request message from the Terminal 1700, the BSM 1723 of the Home SP 1720 sends a request for a purchase item list to the BSM 1713 of the Visited SP 1710 to which the Terminal 1700 is roaming. The contents of the message sent from the BSM 1723 of the Home SP 1720 to the BSM 1713 of the Visited SP 1710 are shown in Table 26 below.

Table 26

Request ID
Terminal ID
Home SP ID
Home SP BSM ID
Visited BSDA ID
Terminal Subscription Type

[0165] Request ID, a first item of Table 26, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID can be used together with the purchase item list request procedure for roaming shown in FIG. 17, and is equal to the Request ID in Tables 16-20 or Tables 21-24. Terminal ID is a unique ID for the terminal for enabling to uniquely identify a terminal. The Terminal ID is used for identifying who makes the purchase item list request for roaming.

[0166] Home SP ID is used for indicating from which service provider the Terminal 1700 that requested the purchase item list for roaming in the Visited SP 1710 has originally received the service. Using this information, the BSM 1713 of the Visited SP 1710 can recognize that the Terminal 1700 that requested the purchase item list for roaming belongs to the service provider with whom its roaming agreement is made. Home SP BSM ID is used for informing the Visited SP 1710 of the entity for a negotiation needed in the purchase item list search process. The BSM 1713 of the Visited SP 1710 responds to the purchase item list request result depending on the Home SP BSM ID.

[0167] Visited BSDA ID is used for providing the Visited SP 1710 with the information indicating in which service area the terminal is currently requesting the service. Terminal Subscription Type is information provided to the Visited SP 1710 to evaluate in which class the terminal that requested the purchase item list for roaming can receive services of the Visited SP 1710. The Terminal Subscription Type can be a class of the service that the roaming-requested Terminal 1700 can receive from the roaming-requested Visited SP 1710 based on the roaming agreement made between the Home SP 1720 and the Visited SP 1710. This can be defined in the form of a roaming allowed class number or code agreed between the two service providers, and its form is not defined in an exemplary embodiment of the present invention.

[0168] In step 1703, the BSM 1713 of the Visited SP 1710 sends a response to the request received in step 1702. The main purpose in step 1703 is to inform the purchase item list requested by the Terminal 1700 using the information received in step 1702. The BSM 1713 of the Visited SP 1710 can optionally provide Roaming Service Allowed Scope as well. The message sent from the BSM 1713 of the Visited SP 1710 to the BSM 1723 of the Home SP 1720 in step 1703 is shown in Table 27 below.

Table 27

Request ID
Roaming Authorization Status
Roaming Service Allowed Scope
Purchase Item List

[0169] Request ID, a first item of Table 27, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID can be used together with the purchase item list request procedure for roaming shown in FIG. 17, and is equal to the Request ID in Tables 16-20 or Tables 21-24. Roaming Authorization Status, which is an item indicating an allowed status of the request, is used for providing the result on the request to the BSM 1723 of the Home SP 1720 of the roaming Terminal 1700 using the information provided in step 1702. Roaming Service Allowed Scope, which is an optional item, is used for allowing a value of the subscription type of the roaming terminal to indicate which reception right the roaming Terminal 1700 will actually have in the Visited SP 1710. Purchase Item List, a list of purchase item IDs, is a list of services that the roaming Terminal 1700 can join in the Visited SP 1710.

[0170] In step 1704, the Home SP 1720 notifies the result on the purchase item list request for roaming received via the Visited SP 1710 in step 1703 to the Terminal 1700. Actually, in step 1704, the BSM 1723 of the Home SP 1720 forwards the message received in step 1703, to the Terminal 1700. After the Home SP 1720 analyzes the request of the terminal in step 1701, if there is no roaming agreement with the Visited SP 1710 in the area where the Terminal 1700 stays, the Home SP 1720 directly proceeds to step 1704 where it fills the contents of Table 27 with a requested process fail and sends it to the Terminal 1700. In this case, the Terminal 1700 fails in the request. Upon receipt of the purchase item list in step 1704, the Terminal 1700 displays the purchase item of its received service guide for the user in such a way of displaying the purchase items in the list through comparison with the purchase items in the received list.

[0171] FIG. 18 is a flowchart illustrating an operation of a BSM 1713 of a Visited SP 1710 according to an exemplary embodiment of the present invention. A description of FIG. 18 will be made with reference to FIG. 17.

[0172] Referring to FIG. 18, in step 1801, the BSM 1713 of the Visited SP 1710 receives a Purchase Item List Request message from a BSM 1723 of a Home SP 1720 of a roaming Terminal 1700, and deciphers the received message. The received message is shown in Table 26. In step 1802, the BSM 1713 of the Visited SP 1710 analyzes Terminal Subscription Type among the contents of the received Purchase Item List Request message.

[0173] After analyzing the contents with the subscription policy of the terminal that requested the purchase item list

in step 1802, the BSM 1713 of the Visited SP 1710 checks the purchase item list subscribable during the roaming in step 1803. If subscription of the roaming-requested Terminal 1700 is insufficient to support the roaming, the BSM 1713 of the Visited SP 1710 generates a message for rejecting the request and delivers the message to the BSM 1723 of the Home SP 1720 in step 1805. If it is determined that the roaming is available with the subscription of the roaming-requested terminal, the BSM 1713 of the Visited SP 1710 generates a purchase item list and sends a response message to the BSM 1723 of the Home SP 1720 in step 1804. The contents of this message are shown in Table 27.

[0174] FIG. 19 is a diagram illustrating an operation of a BSM 1723 of a Home SP 1720 according to the fourth embodiment of the present invention. A description of FIG. 19 will be made with reference to FIG. 17.

[0175] Referring to FIG. 19, in step 1901, the BSM 1723 of the Home SP 1720 receives a Purchase Item List Request message for roaming from a roaming Terminal 1700, and deciphers the received message. The message received by the Home SP 1720 is shown in Table 25. Using the deciphered message, the BSM 1723 of the Home SP 1720 first determines in step 1902 whether there is a roaming agreement with a Visited SP 1710 where the Terminal 1700 that requested the purchase item list during the roaming stays. If there is no roaming agreement, the BSM 1723 of the Home SP 1720 proceeds to step 1909 where it performs a roaming-unavailable process. In step 1909, the BSM 1723 of the Home SP 1720 can include even the cause of the roaming unavailability when necessary while notifying Roaming Unavailable subscription.

[0176] However, if there is a roaming agreement, the BSM 1723 of the Home SP 1720 retrieves subscription of the corresponding Terminal 1700 in step 1903, and determines in step 1904 whether the retrieved subscription of the Terminal 1700 is a Roaming Allowable subscription.

[0177] If the received subscription of the Terminal 1700 is a Roaming Unsupported subscription, the BSM 1723 of the Home SP 1720 proceeds to step 1909 to inform that the corresponding subscription is a Roaming Unavailable subscription. In step 1909, the BSM 1723 of the Home SP 1720 can also include the cause of the roaming unavailability when necessary while notifying the Roaming Unavailable subscription.

[0178] If the retrieved subscription is Roaming Supported subscription, the BSM 1723 of the Home SP 1720 sends a Purchase Item List Request message for roaming to a BSM 1713 of the Visited SP 1710 in step 1905. The contents of this message are shown in Table 26. After sending the request message, the BSM 1723 of the Home SP 1720 waits for a response from the Visited SP 1710 in step 1906. Upon receipt of the response to the request, the BSM 1723 of the Home SP 1720 deciphers the received response message in step 1907, and generates a message indicating the result on the purchase item list request for roaming and delivers the generated message to the Terminal 1700 in step 1908.

[0179] FIG. 20 is a flowchart illustrating an operation of a Terminal 1700 according to an exemplary embodiment of the present invention. A description of FIG. 20 will be made with reference to FIG. 17.

[0180] Referring to FIG. 20, in step 2001, the Terminal 1700 sends a Purchase Item List Request message for roaming to a BSM 1723 of its Home SP 1720 to determine a list of purchase items for which the Terminal 1700 can subscribe in a corresponding area while performing the roaming. Thereafter, in step 2002, the Terminal 1700 waits for a response from the BSM 1723 of the Home SP 1720. The contents of the transmitted message are shown in Table 25. Upon receipt of the response message from the BSM 1723 of the Home SP 1720, the Terminal 1700 compares the received purchase item list with the purchase items in its received service guide, and displays the purchase item in the list in step 2003. Here, the message received by the Terminal 1700 is shown in Table 27.

[0181] A description will now be made of a purchase item list request procedure for roaming according to an exemplary embodiment of the present invention.

[0182] FIG. 21 is a signaling diagram illustrating a purchase item list request procedure for roaming according to an exemplary embodiment of the present invention. Before a description of each step in the purchase item list request procedure for roaming is given, each entity of FIG. 21 will first be described. BSAs 2124 and 2114 in a Home SP 2120 and a Visited SP 2110 are equal in function to the BSA 102 of FIG. 1, so they are separately shown to differentiate the BSA in the Home SP 2120 from the BSA in the Visited SP 2110 during roaming. Similarly, BSMs 2123 and 2113 have the same function as that of the BSM 104 of FIG. 1, BSDAs 2122 and 2112 have the same function as that of the BSDA 103 of FIG. 1, and group entities 2121 and 2111, each composed of BDS-SD, BDS and/or IN, have the same function as the group entity of the BDS-SD 111, the BDS 112 and/or the IN 113 of FIG. 1. A Terminal 2100 has the same function as that of the Terminal 105 of FIG. 1. The above-mentioned entities are not all used in the purchase item list request procedure for roaming according to an exemplary embodiment of the present invention, so the entities used in the purchase item list request procedure for roaming will be described. The procedure shown in FIG. 21 can be optionally used during roaming, and it can be used between steps 802 and 803 of an exemplary embodiment of the present invention.

[0183] Referring to FIG. 21, in step 2101, using the information shown in Table 11 acquired through reception of a service guide, the Terminal 2100 generates a Purchase Item List Request message for requesting information indicating which purchase items the Terminal 2100 can join during the roaming, and sends the generated message to the BSM 2113 of the Visited SP 2110. The contents of the Purchase Item List Request message generated by the Terminal 2100 in step 2101 are shown in Table 28 below.

Table 28

Request ID
Terminal ID
Home SP ID
Home SP BSM ID

[0184] Request ID, a first item of Table 28, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID can be used together with the purchase item list request procedure for roaming shown in FIG. 21, and is equal to the Request ID in Tables 16-20. Terminal ID is a unique ID for the terminal for enabling to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request.

[0185] Home SP ID is an identifier used for allowing the roaming Terminal 2100 to inform the Visited SP 2110 who it's Home SP 2120 is. Using this information, the Visited SP 2110 can determine to which entity the roaming-requested Terminal 2100 originally belongs, and can also determine a roaming relationship with the corresponding entity. Here, when the BSM 2113 of the Visited SP 2110 determines from the Home SP ID that there is no roaming agreement made with the BSM 2113 itself, the BSM 2113 directly proceeds to step 2104 where it can notify a roaming unavailability to the Terminal 2100.

[0186] Home SP BSM ID is used for informing the Visited SP 2110 of the entity that actually makes a negotiation on a roaming service registration procedure with the identifier of the BSM 2123 used by the Home SP 2120. Finally, Purchase item ID is used for indicating the service that the roaming user desires to receive. For the terminal that made the purchase item list request for roaming in step 2101, the BSM 2113 of the Visited SP 2110 can additionally perform an authentication process on the terminal, and this can be performed spontaneously by the BSM 2113 of the Visited SP 2110, or can be performed through a connection with the BSM 2123 of the Home SP 2120 or through the third authentication entity. Because the authentication process is not related to the basis of the present invention, a description thereof will be omitted herein for clarity and conciseness.

[0187] In step 2102, for the purchase item list request for roaming received from the Terminal 2100 in step 2101, the BSM 2113 of the Visited SP 2110 sends a request for subscription information for the corresponding terminal to the BSM 2123 of the Home SP 2120. The contents of the message sent from the BSM 2113 of the Visited SP 2110 to the BSM 2123 of the Home SP 2120 in step 2102 are shown in Table 29 below.

Table 29

Request ID
Terminal ID
Visited SP ID
Visited SP BSM ID

[0188] Request ID, a first item of Table 29, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID can be used together with the purchase item list request procedure for roaming shown in FIG. 21, and is equal to the Request ID in Tables 16-20. Terminal ID is a unique ID for the terminal for enabling to uniquely identify a terminal. The Terminal ID is used for identifying who makes the roaming registration request. Visited SP ID is used by the Visited SP 2110 to provide its own informing to the BSM 2123 of the Home SP 2120 of the terminal that requested the purchase item list when the terminal is roaming thereto. Visited SP BSM ID is used by the Visited SP 2110 to provide the BSM 2123 of the Home SP 2120 with the information indicating the entity with which a roaming-related negotiation is to be made. This is because the Visited SP 2110 can have several BSMs.

[0189] In step 2103, the BSM 2123 of the Home SP 2120 responds to the Terminal subscription information request received in step 2102. Table 30 below shows the contents of the message sent from the BSM 2123 of the Home SP 2120 to the BSM 2113 of the Visited SP 2110.

Table 30

Request ID
Roaming Authorization Status
Terminal Subscription Type

[0190] Request ID, a first item of Table 30, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID can be used together with the purchase item list request procedure for roaming shown in FIG. 21, and is equal to the Request ID in Table 16-20. Roaming Authorization Status is used for allowing the Home SP 2120 to determine whether the roaming is authorized by retrieving subscription of the Terminal 2100 that requested the purchase item list for roaming in the Visited SP 2110 using the Terminal ID received in step 2103, and to provide the results to the Visited SP 2110.

[0191] Terminal Subscription Type is information provided for allowing the Visited SP 2110 to evaluate which reception right the roaming Terminal 2100 will actually have in the Visited SP 2110. The Terminal Subscription Type can be a class of the service that the roaming-requested Terminal 2100 can receive from the roaming-requested Visited SP 2110 based on the roaming agreement made between the Home SP 2120 and the Visited SP 2110. This can be defined in the form of a roaming allowed class number or code agreed between the two service providers, and its form is not defined in an exemplary embodiment of the present invention.

[0192] In step 2104, the Visited SP 2110 sends a response to the received purchase item list request for roaming to the Terminal 2100. The contents of the message sent from the BSM 2113 of the Visited SP 2110 to the Terminal 2100 in step 2104 are shown in Table 31 below.

Table 31

Request ID
Roaming Authorization Status
Purchase Item List

[0193] Request ID, a first item of Table 31, is an identifier given to consistently identify and manage one roaming registration request procedure. The Request ID is an identifier generated for allowing a terminal to uniquely identify its own roaming registration request. The Request ID can be used together with the purchase item list request procedure for roaming shown in FIG. 21, and is equal to the Request ID in Tables 16-20. Roaming Authorization Status is used for allowing the Home SP 2120 to inform the Terminal 2100 of the result on the purchase item list request for roaming, using the information provided in step 2103. Purchase Item List, a list of purchase item IDs, is a list of services that the roaming Terminal 2100 can join in the Visited SP 2110.

[0194] In step 2104, upon receipt of the purchase item list, the Terminal 2100 displays the purchase item of its received service guide for the user in such a way of displaying the purchase items in the list through comparison with the purchase items in the received list.

[0195] FIG. 22 is a flowchart illustrating an operation of a BSM 2113 of a Visited SP 2110 according to an exemplary embodiment of the present invention. A description of FIG. 22 will be made with reference to FIG. 21.

[0196] Referring to FIG. 22, in step 2201, the BSM 2113 of the Visited SP 2110 receives a message for a purchase item list request for roaming from a roaming Terminal 2100, and deciphers the received request message. The contents of the received message are shown in Table 28. In step 2202, the BSM 2113 of the Visited SP 2110 determines whether the Terminal 2100 that requested the purchase item list for roaming using the contents of the deciphered message is a terminal of the service provider having a roaming agreement with the terminal. If the Terminal 2100 belongs to the service provider having no roaming agreement, then the BSM 2113 of the Visited SP 2110 proceeds to step 2208 where it transmits a Roaming Unavailable Response message to the Terminal 2100. In step 2208, the BSM 2113 of the Visited SP 2110 can include even the cause of the roaming unavailability when necessary while notifying the Roaming Unavailable message.

[0197] However, if the Terminal 2100 belongs to the service provider having the roaming agreement therewith, the BSM 2113 of the Visited SP 2110 transmits a Terminal Request message to a BSM 2123 of a Home SP 2120 of the terminal that requested the purchase item list for roaming in step 2203. Here, the contents of the transmitted message are shown in Table 29. Thereafter, in step 2204, the BSM 2113 of the Visited SP 2110 waits for a response message from the BSM 2123 of the Home SP 2120 of the roaming-requested Terminal 2100. In step 2205, the BSM 2113 of the Visited SP 2110 receives the response message from the BSM 2123 of the Home SP 2120, and deciphers the received

response message. The contents of the received response message are shown in Table 30.

[0198] After analyzing the contents of the received message, the BSM 2113 of the Visited SP 2110 determines in step 2206 whether it is authorized to provide the purchase item list for roaming to the Terminal 2100. If the BSM 2113 of the Visited SP 2110 is not authorized to do so, it transmits a Roaming Unavailable message to the Terminal 2100 in step 2208. In step 2208, the BSM 2113 of the Visited SP 2110 can include even the cause of the roaming unavailability when necessary while notifying the Roaming Unavailable message. However, if the BSM 2113 of the Visited SP 2110 is authorized to do so, it generates a purchase item list for roaming using the subscription information of the Terminal 2100, and transmits the purchase item list to the Terminal 2100 in step 2207.

[0199] FIG. 23 is a flowchart illustrating an operation of a BSM 2123 of a Home SP 2120 according to an exemplary embodiment of the present invention. A description of FIG. 23 will be made with reference to FIG. 21.

[0200] Referring to FIG. 23, in step 2301, the BSM 2123 of the Home SP 2120 receives a Terminal Subscription Information Request message for the terminal that requested a purchase item list request for roaming from a BSM 2113 of a Visited SP 2110, and deciphers the received message. The contents of the message received by the Home SP 2120 are shown in Table 29. In step 2302, the BSM 2123 of the Home SP 2120 retrieves subscription of the Terminal 2100 that requested the purchase item list for roaming in the Visited SP 2110. Thereafter, the BSM 2123 of the Home SP 2120 determines in step 2303 whether the Terminal 2100 that requested the purchase item list for roaming is allowed to receive the roaming service. If the Terminal 2100 is allowed to receive the roaming service, the BSM 2123 of the Home SP 2120 transmits a message including the contents shown in Table 30 where subscription of the Terminal 2100 is included, to the Visited SP 2110 in step 2304. However, if the Terminal 2100 is not allowed to receive the roaming service, the BSM 2123 of the Home SP 2120 transmits a Roaming Unavailable message to the Visited SP 2110 in step 2305.

[0201] FIG. 24 is a flowchart illustrating an operation of a Terminal 2100 according to an exemplary embodiment of the present invention. A description of FIG. 24 will be made with reference to FIG. 21.

[0202] Referring to FIG. 24, in step 2401, the Terminal 2100 sends a Purchase Item List Request message for roaming to a BSM 2113 of a Visited SP 2110 to determine a list of purchase items for which the Terminal 2100 can subscribe in a corresponding area while performing the roaming. The contents of the sent message are shown in Table 28. In step 2402, the Terminal 2100 waits for a response from the BSM 2113 of the Visited SP 2110. Thereafter, in step 2403, the Terminal 2100 receives the response message from the BSM 2113 of the Visited SP 2110, compares the received purchase item list with the purchase items in its received service guide, and displays the purchase item in the list. Here, the message received by the Terminal 2100 is shown in Table 31.

[0203] As can be understood from the foregoing description, exemplary embodiments of the present invention provide a procedure and method for enabling roaming in a mobile broadcasting system, and the procedure provides a communication procedure between the home service provider for which the user first subscribed and the visited service provider having a roaming agreement with the home serving provider. In addition, exemplary embodiments of the present invention provide the message and procedure capable of supporting various charging systems for the roaming service requested by the user.

[0204] While the invention has been shown and described with reference to a certain exemplary embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined by the appended claims.

[0205] The following is a list of further preferred embodiments of the invention:

Embodiment 1: A roaming service method in a mobile broadcasting system, the method comprising:

receiving, by a terminal, a service guide from a corresponding visited service provider (Visited SP) when the terminal moves to a roaming area;
transmitting, by the terminal, a roaming request message for requesting a purchase item allowable for individual services to a home service provider (Home SP) based on the received service guide;
upon receipt of the roaming request message, negotiating, by the Home SP, roaming availability and allowable scope for the individual services with the Visited SP where the terminal is located, based on the roaming request message; and
transmitting, by the Home SP, the roaming availability and allowable scope for the individual services, negotiated with the Visited SP, to the terminal.

Embodiment 2: The roaming service method of embodiment 1, wherein the roaming request message further includes an allowability request of a particular service selected by the terminal.

Embodiment 3: The roaming service method of embodiment 1, wherein the negotiating of the roaming availability and allowable scope comprises:

transmitting, by the Home SP, a message including a subscription type of the terminal to the Visited SP, for roaming registration; and
determining, by the Visited SP, roaming availability and allowable scope for the individual services based on the subscription type, and transmitting the result to the Home SP.

5

Embodiment 4: The roaming service method of embodiment 1, further comprising:

transmitting, by the terminal, at least one of agreement and disagreement on the allowable scope for the individual services to the Visited SP; and
if the terminal agrees, transmitting, by the Visited SP, an enciphering key for receiving the agreed service.

10

Embodiment 5: The roaming service method of embodiment 1, further comprising:

transmitting, by the terminal, at least one of agreement and disagreement on the allowable scope for the individual services to the Home SP; and
sending, by the Home SP, a request for an enciphering key for receiving the service agreed by the terminal to the Visited SP, receiving the enciphering key from the Visited SP, and transmitting the received enciphering key to the terminal.

15

Embodiment 6: The roaming service method of embodiment 4, wherein the enciphering key is a long-term key.

20

Embodiment 7: The roaming service method of embodiment 1, further comprising transmitting, by the Home SP, charging information for a roaming service to the terminal.

25

Embodiment 8: A roaming service method in a mobile broadcasting system, the method comprising:

receiving, by a terminal, a service guide from a corresponding visited service provider (Visited SP) when the terminal moves to a roaming area;
transmitting, by the terminal, a roaming request message for requesting a purchase item allowable for the individual services to a visited service provider (Visited SP) based on the received service guide;
upon receipt of the roaming request message, determining by the Visited SP whether a roaming service of the terminal is authorized from a home service provider (Home SP) for which the terminal has subscribed, based on the roaming request message; and
verifying, by the Visited SP, availability of the roaming service of the terminal and an allowable scope for the individual roaming services, and transmitting the result to the terminal.

30

35

Embodiment 9: The roaming service method of embodiment 8, wherein the transmitting of the roaming request message further comprises including an allowability request of a service selected by the terminal in the roaming request message.

40

Embodiment 10: The roaming service method of embodiment 8, wherein the determining of whether the roaming service of the terminal is authorized comprises:

transmitting, by the Visited SP, a message including a subscription type of the terminal to the Home SP, for roaming registration; and
determining, by the Home SP, roaming availability based on the subscription type, and transmitting the determined roaming availability to the Home SP.

45

Embodiment 11: The roaming service method of embodiment 8, further comprising:

50

transmitting, by the terminal, at least one of agreement and disagreement on the allowable scope for the individual services to the Visited SP; and
if the terminal agrees, transmitting, by the Visited SP, an enciphering key for receiving the agreed service.

55

Embodiment 12: The roaming service method of embodiment 11, wherein the enciphering key is a long-term key.

Embodiment 13: The roaming service method of embodiment 8, further comprising transmitting, by the Visited SP, charging information for a roaming service to the terminal.

Embodiment 14: A mobile broadcasting system comprising:

a home service provider (Home SP) for, upon receipt of a roaming request message from a terminal, negotiating roaming availability and allowable scope for individual roaming services with a visited service provider (Visited SP) where the terminal is located, based on the roaming request message;
the Visited SP for transmitting the negotiated roaming availability and allowable scope for the individual roaming services to the terminal; and
the terminal for verifying the received roaming availability and allowable scope for the individual roaming services, and receiving an enciphering key from the at least one of the Home SP and the Visited SP.

Embodiment 15: The mobile broadcasting system of embodiment 14, wherein the Home SP further transmits charging information for a roaming service to the terminal.

Embodiment 16: The mobile broadcasting system of embodiment 14, wherein the terminal further includes an allowability request of a service selected by the terminal in the roaming request message.

Embodiment 17: The mobile broadcasting system of embodiment 15, wherein the enciphering key is a long-term key.

Embodiment 18: A mobile broadcasting system comprising:

a visited service provider (Visited SP) for, upon receipt of a roaming request message from a terminal, inquiring of a home service provider (Home SP) for which the terminal has subscribed, regarding availability of the roaming service, based on the roaming request message, verifying the roaming availability and allowable scope for individual roaming services, and transmitting the result to the terminal;
the Home SP for, upon receipt of a request for the roaming service of the terminal from the Visited SP, determining whether to authorize the roaming service of the terminal, and transmitting the result to the Visited SP; and
the terminal for verifying the roaming availability and allowable scope for the individual roaming service, and receiving an enciphering key from the at least one of the Home SP and the Visited SP.

Embodiment 19: The mobile broadcasting system of embodiment 18, wherein the terminal further includes an allowability request of a service selected by the terminal in the roaming request message before transmission.

Embodiment 20: The mobile broadcasting system of embodiment 18, wherein the Visited SP further transmits charging information for a roaming service to the terminal.

Embodiment 21: The mobile broadcasting system of embodiment 18, wherein the enciphering key is a long-term key.

Claims

1. A roaming service method in a terminal of a mobile broadcasting system, the method comprising:

transmitting a roaming request message for requesting a purchase item allowable for individual services to at least one of its home service provider (Home SP) and a visited service provider (Visited SP) based on a service guide received from the Visited SP when the terminal moves to a roaming area;
receiving a roaming response message from the at least one of the Home SP and the Visited SP, verifying roaming availability and allowable scope for each individual service, and transmitting at least one of agreement and disagreement to the Home SP or the Visited SP; and
if the verified roaming condition is agreed, receiving an enciphering key from the at least one of the Home SP and the Visited SP.

2. The roaming service method of claim 1, wherein the terminal further includes an allowability request of a service selected in the roaming request message.

3. The roaming service method of claim 1, wherein the roaming response message further includes charging information for a roaming service to the terminal.

4. The roaming service method of claim 1, wherein the enciphering key is a long-term key.

5. A terminal in a mobile broadcasting system, comprising:

a controller for generating a roaming request message for requesting a purchase item allowable for individual services based on a service guide received from a corresponding visited service provider (Visited SP), when the terminal moves to a roaming area, and deciphering a response message to the roaming request; and
 a transceiver for transmitting the generated roaming request message to at least one of a home service provider (Home SP) and the Visited SP, and receiving a roaming response message from the at least one of the Home SP and the Visited SP and transmitting the received roaming response message to the controller.

6. The terminal of claim 5, wherein the controller further includes an allowability request of a service selected in the roaming request message.

7. The terminal of claim 5, wherein the roaming response message further includes charging information for a roaming service to the terminal.

8. A mobile broadcasting system comprising:

a home service provider (Home SP);
 a visited service provider (Visited SP); and
 a terminal for at least one of verifying roaming availability and allowable scope for individual roaming services,

wherein the HOME SP negotiates roaming availability and allowable scope for individual roaming services with a visited service provider (Visited SP) where the terminal is located, based on the roaming request message, upon receipt of a roaming request message from a terminal,

the Visited SP transmits the negotiated roaming availability and allowable scope for the individual roaming services to the terminal, and

the terminal receives an enciphering key from the at least one of the Home SP and the Visited SP.

9. The mobile broadcasting system of claim 8, wherein the Home SP further transmits charging information for a roaming service to the terminal.

10. The mobile broadcasting system of claim 8, wherein the terminal further includes an allowability request of at least one of a service selected by the terminal in the roaming request message and a service selected by the terminal in the roaming request message before transmission.

11. The mobile broadcasting system of claim 8, wherein the enciphering key is a long-term key.

12. The mobile broadcasting system of claim 8, wherein the Visited SP further transmits charging information for a roaming service to the terminal.

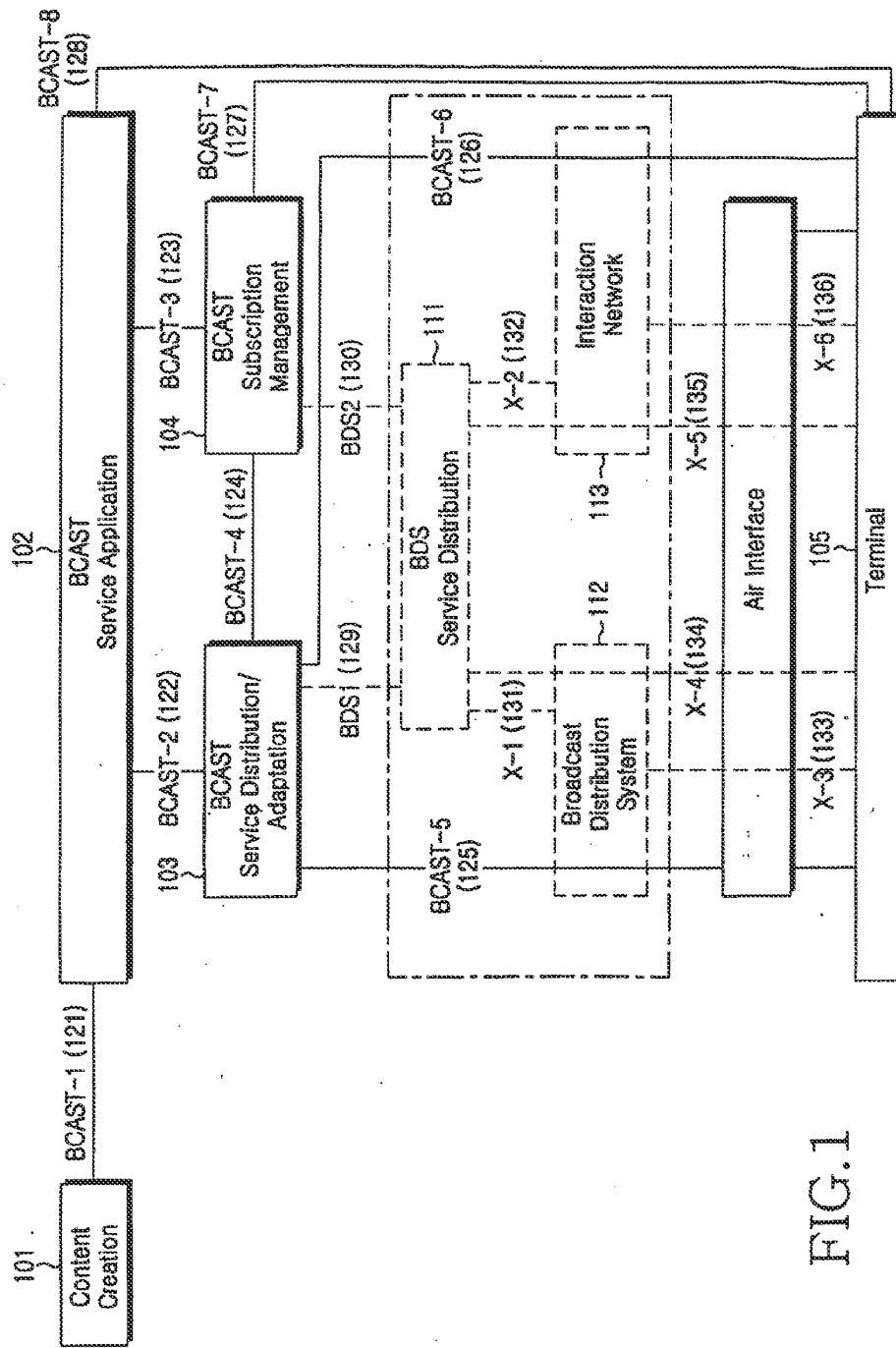


FIG.1

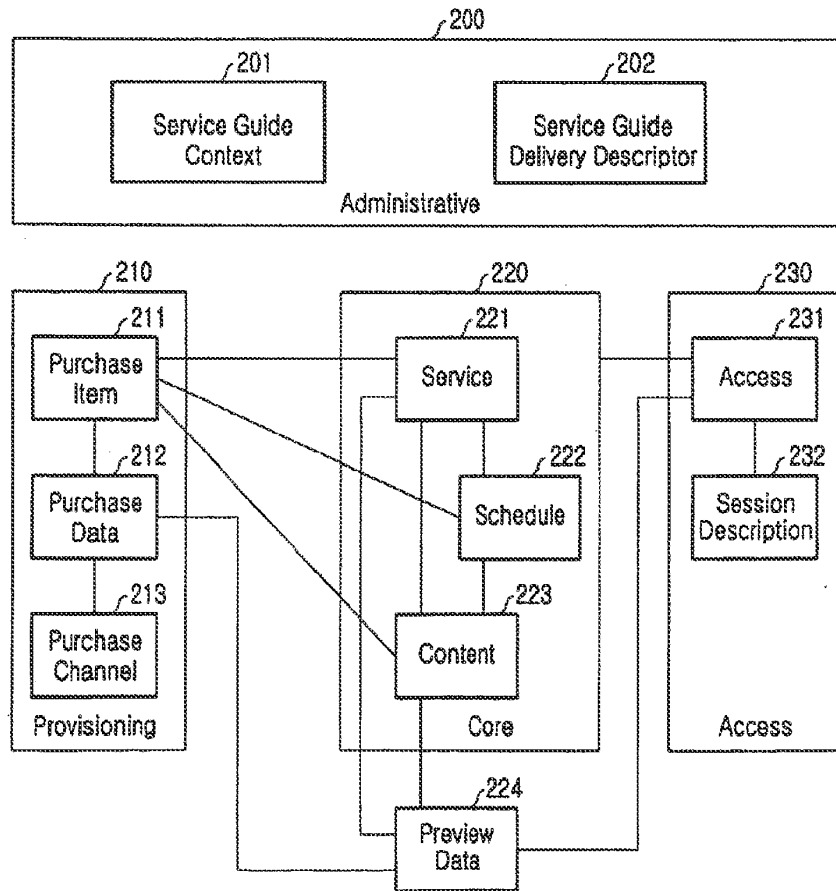


FIG.2

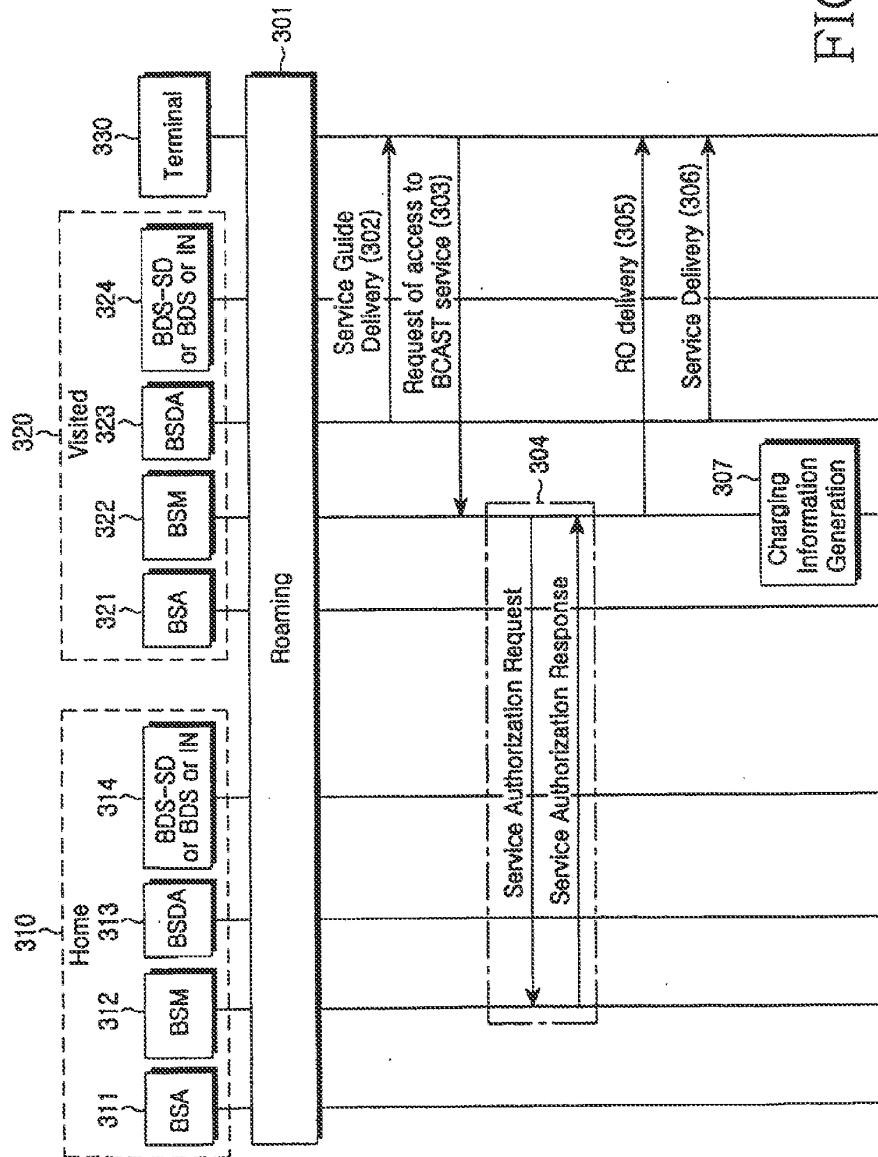


FIG.3

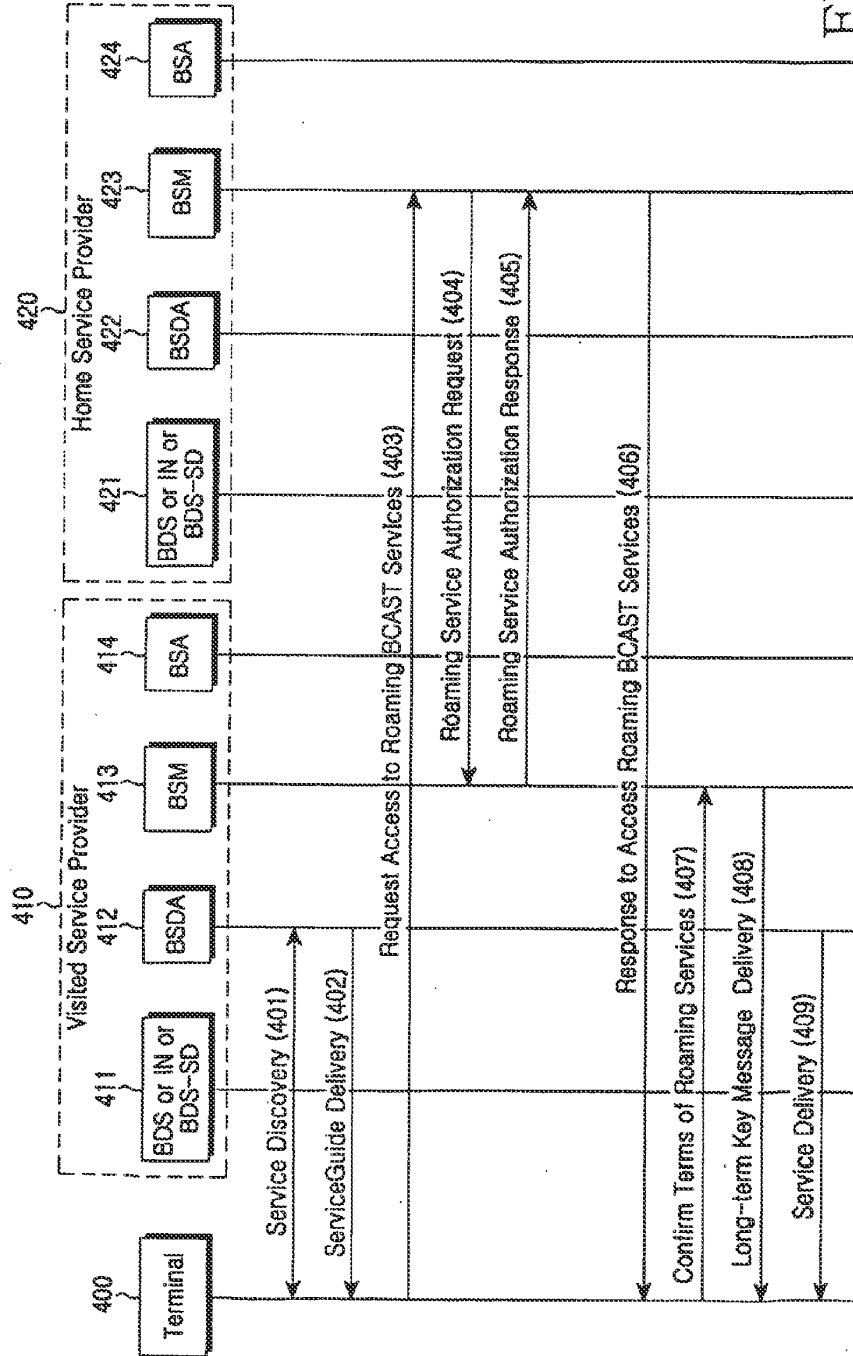


FIG.4

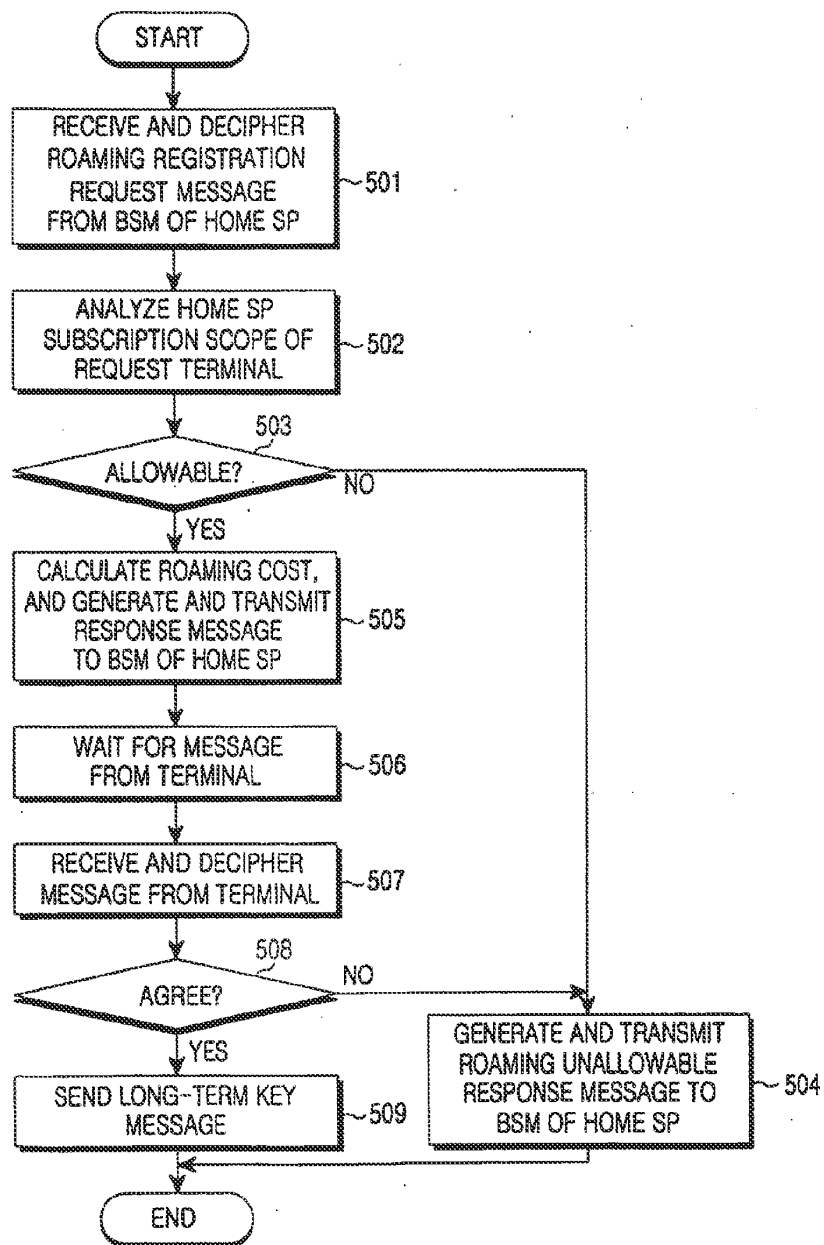
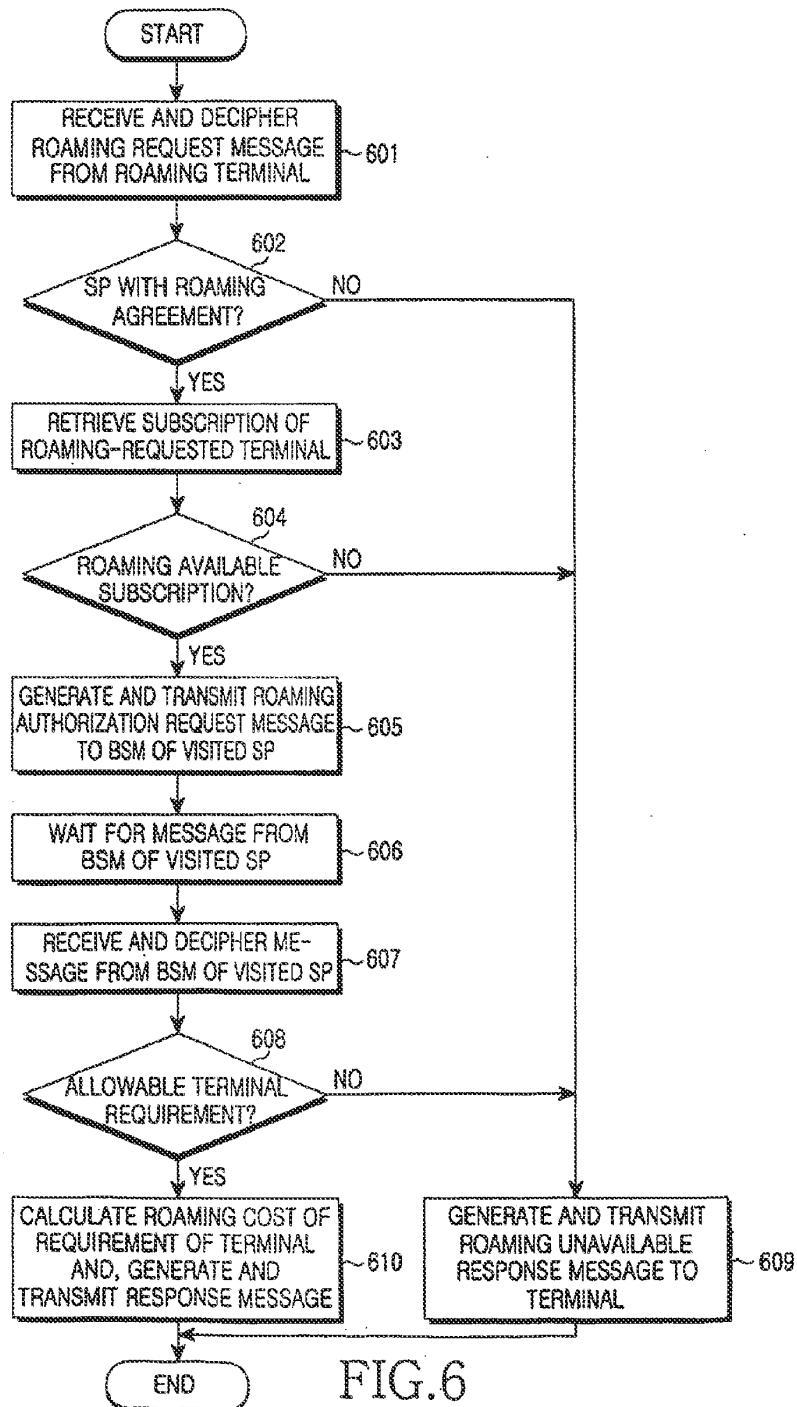


FIG.5



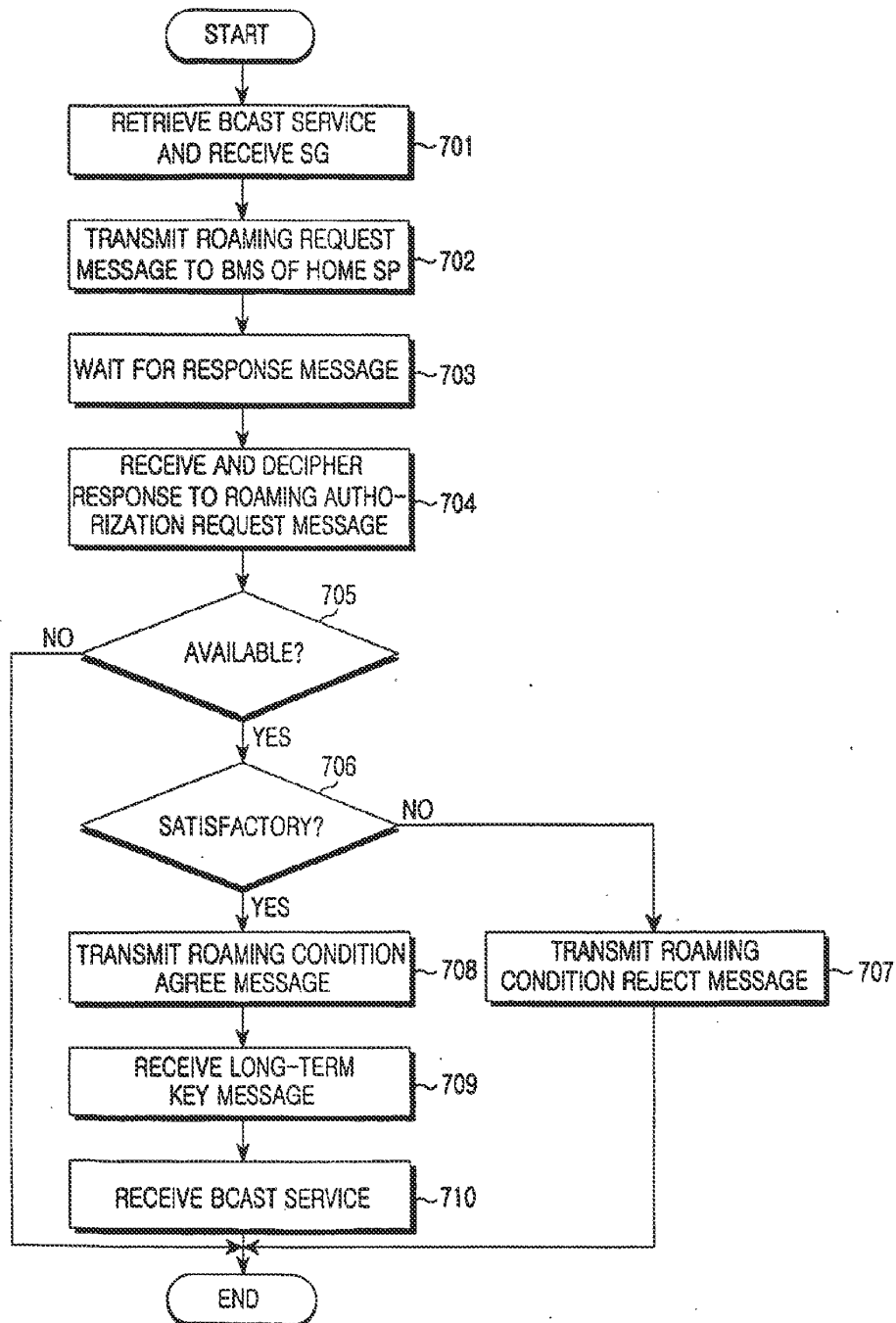


FIG.7

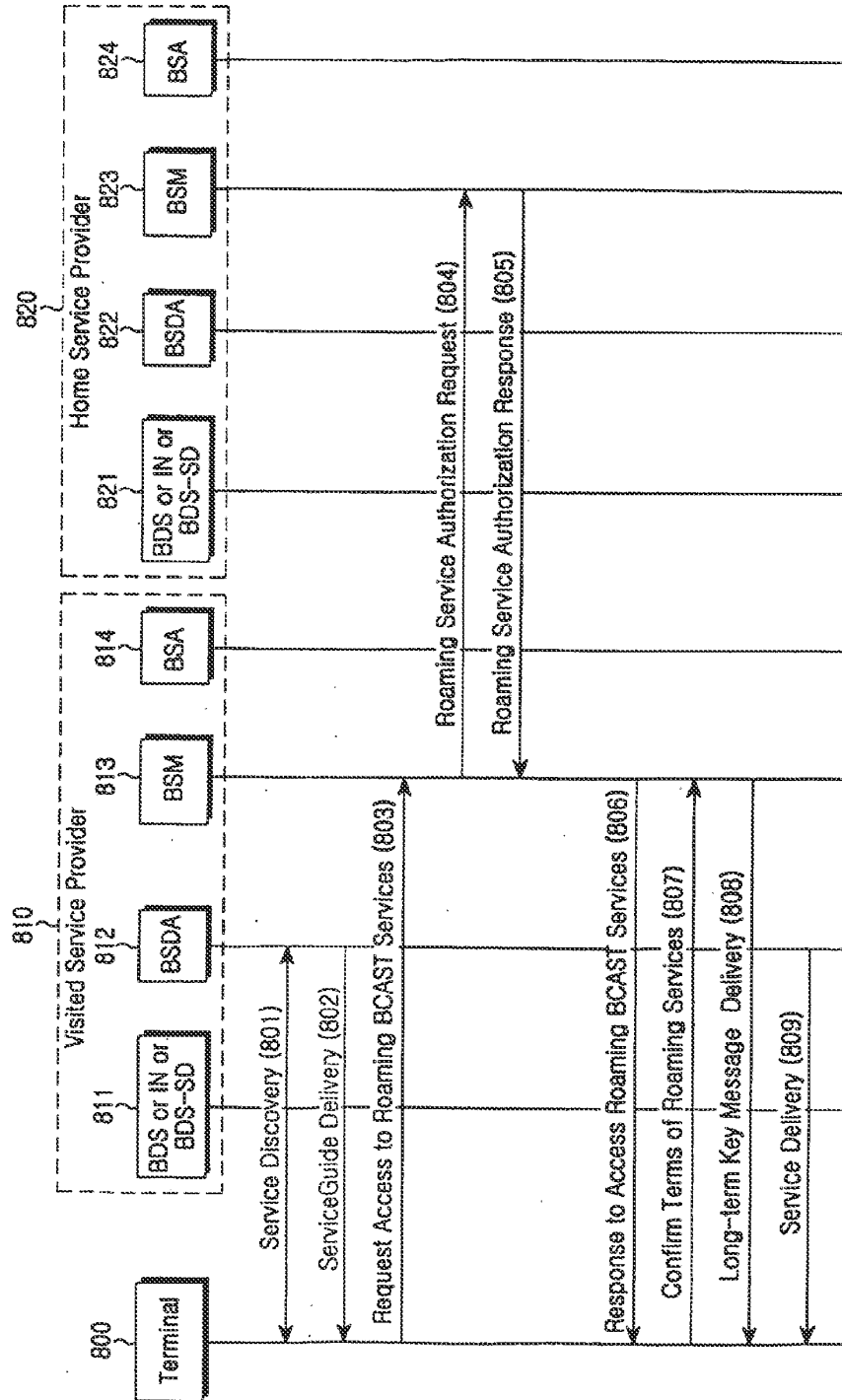
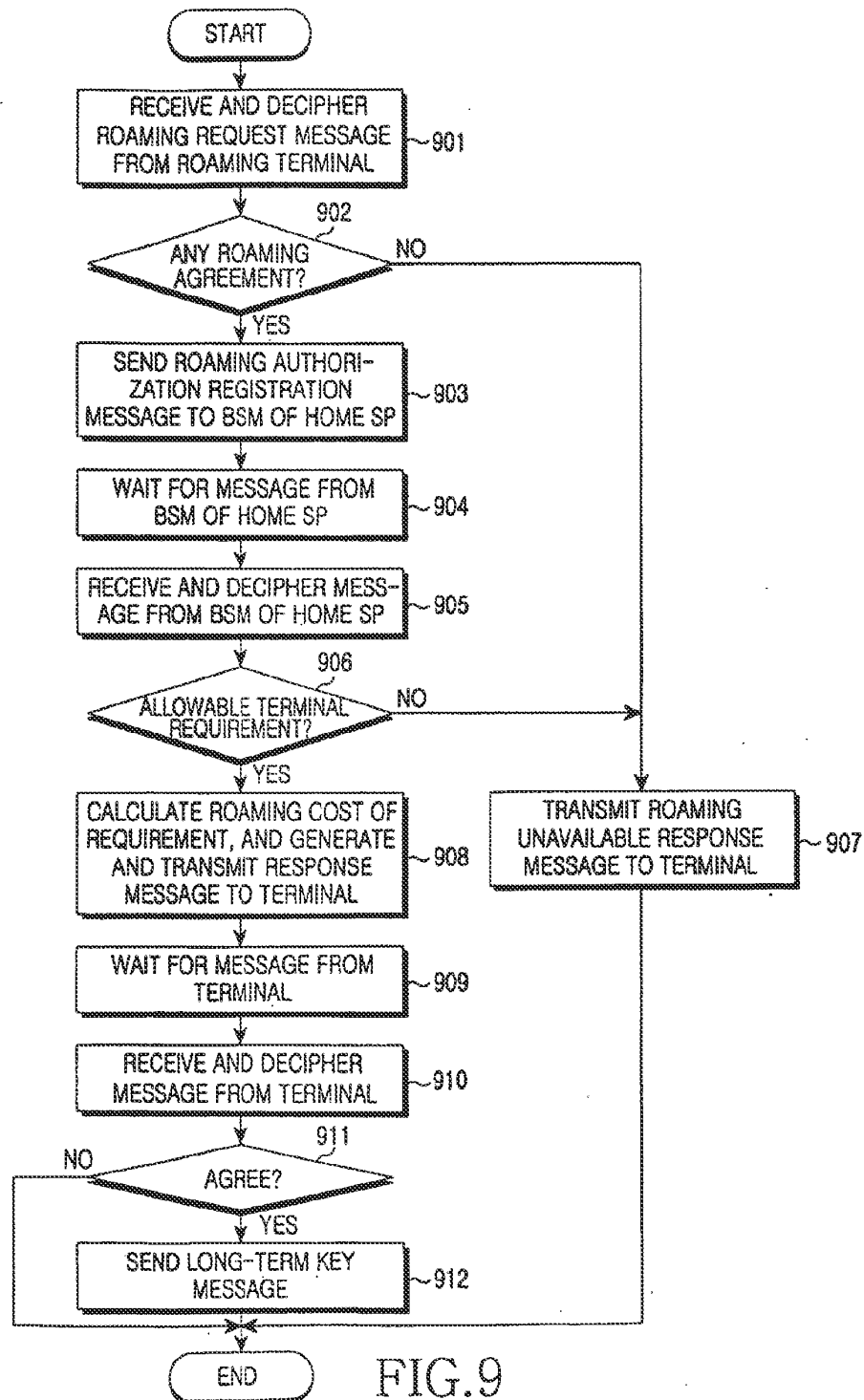


FIG.8



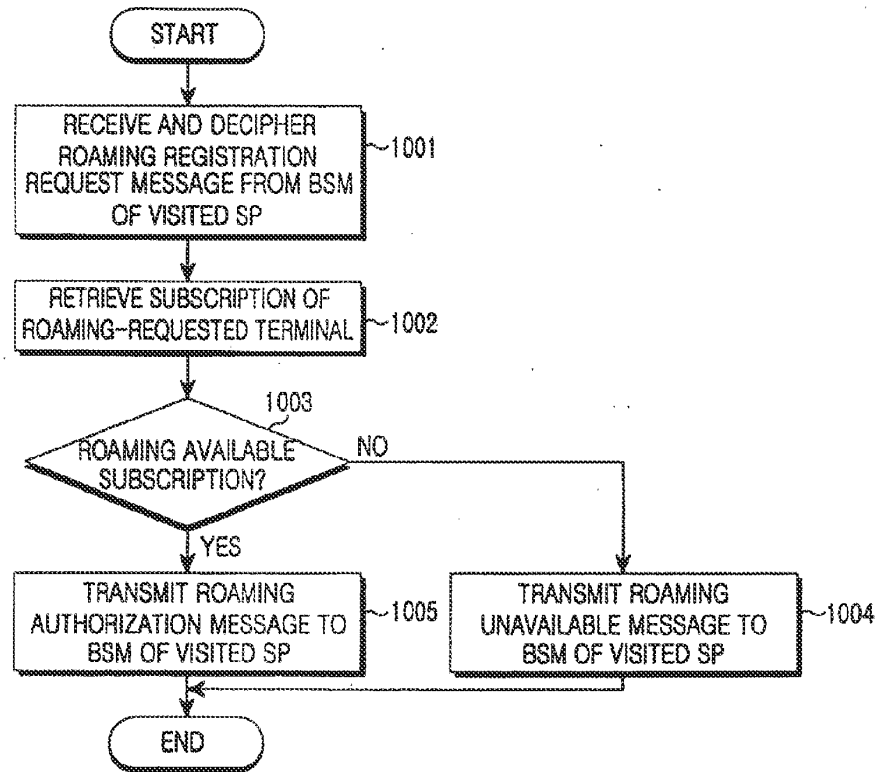


FIG.10

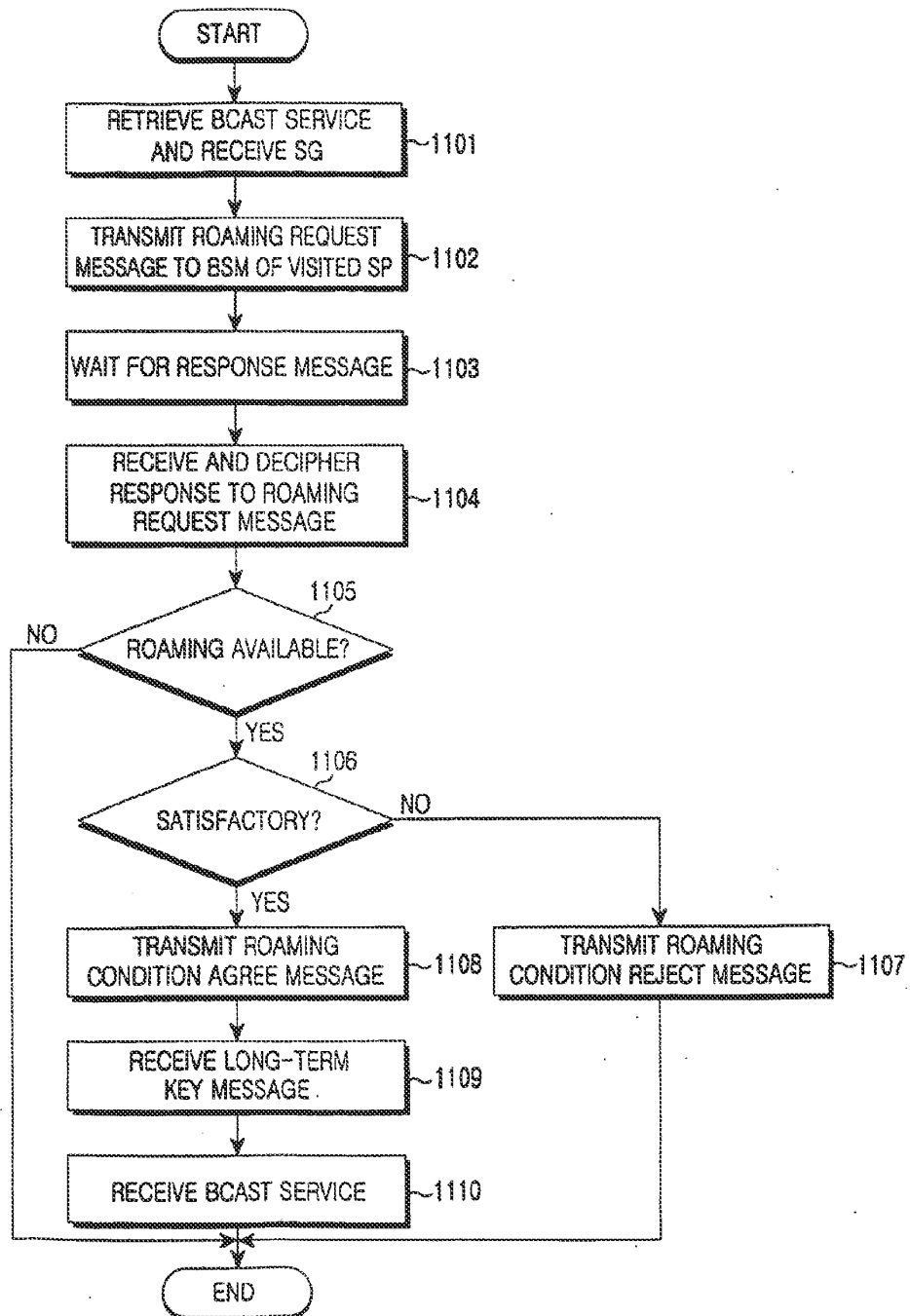


FIG.11

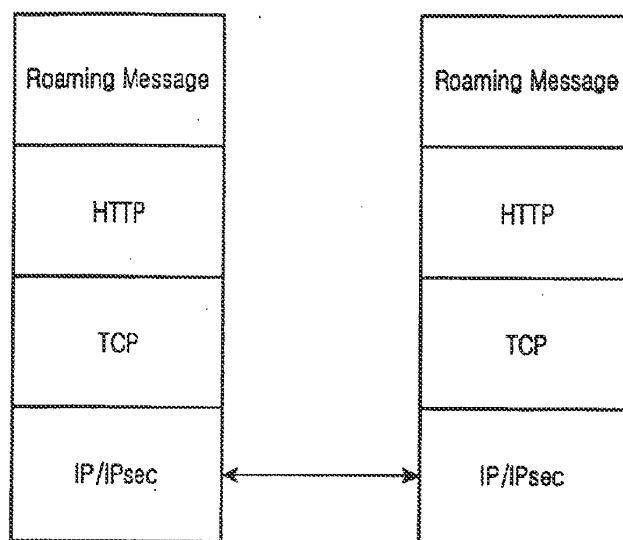


FIG.12

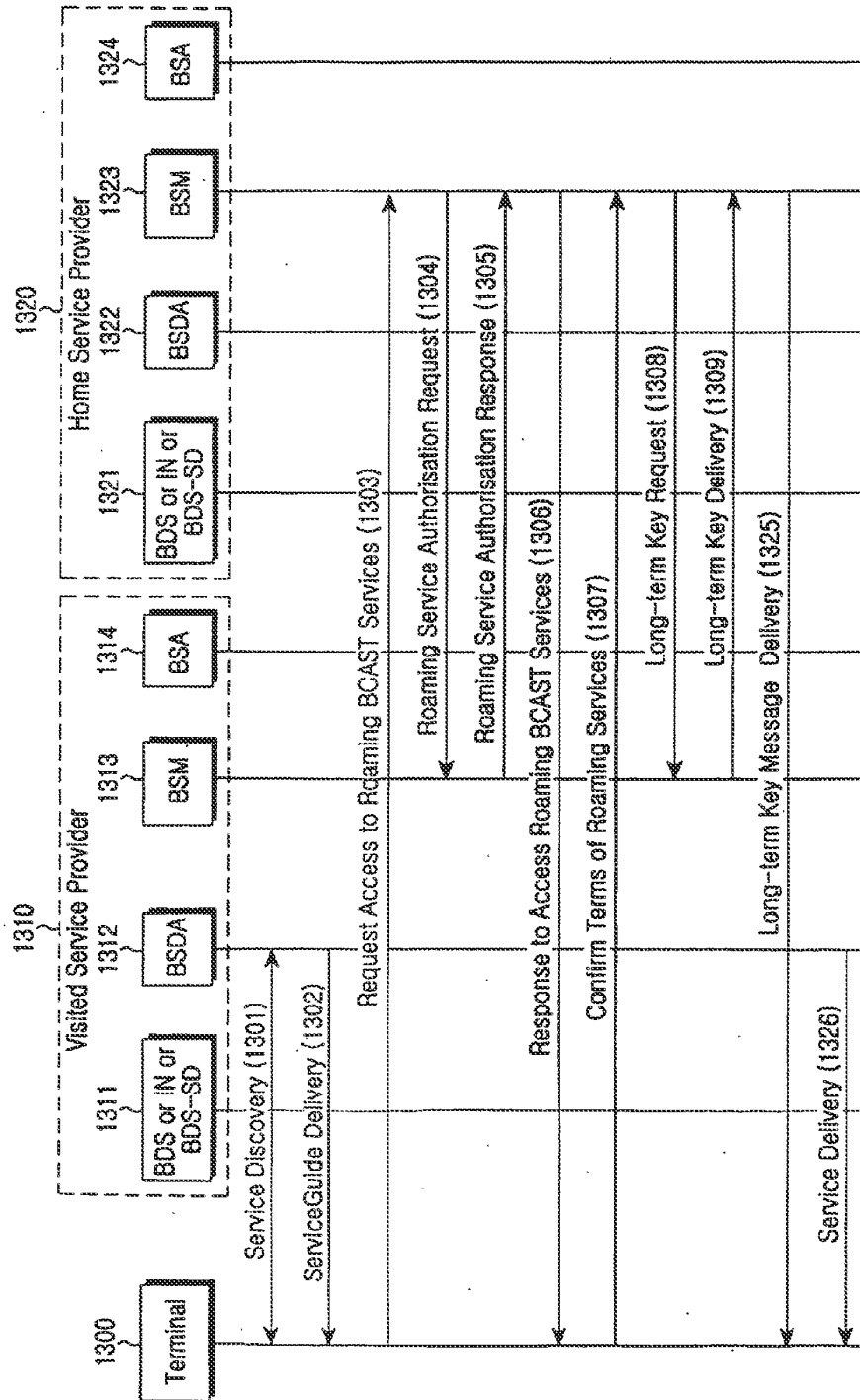


FIG.13

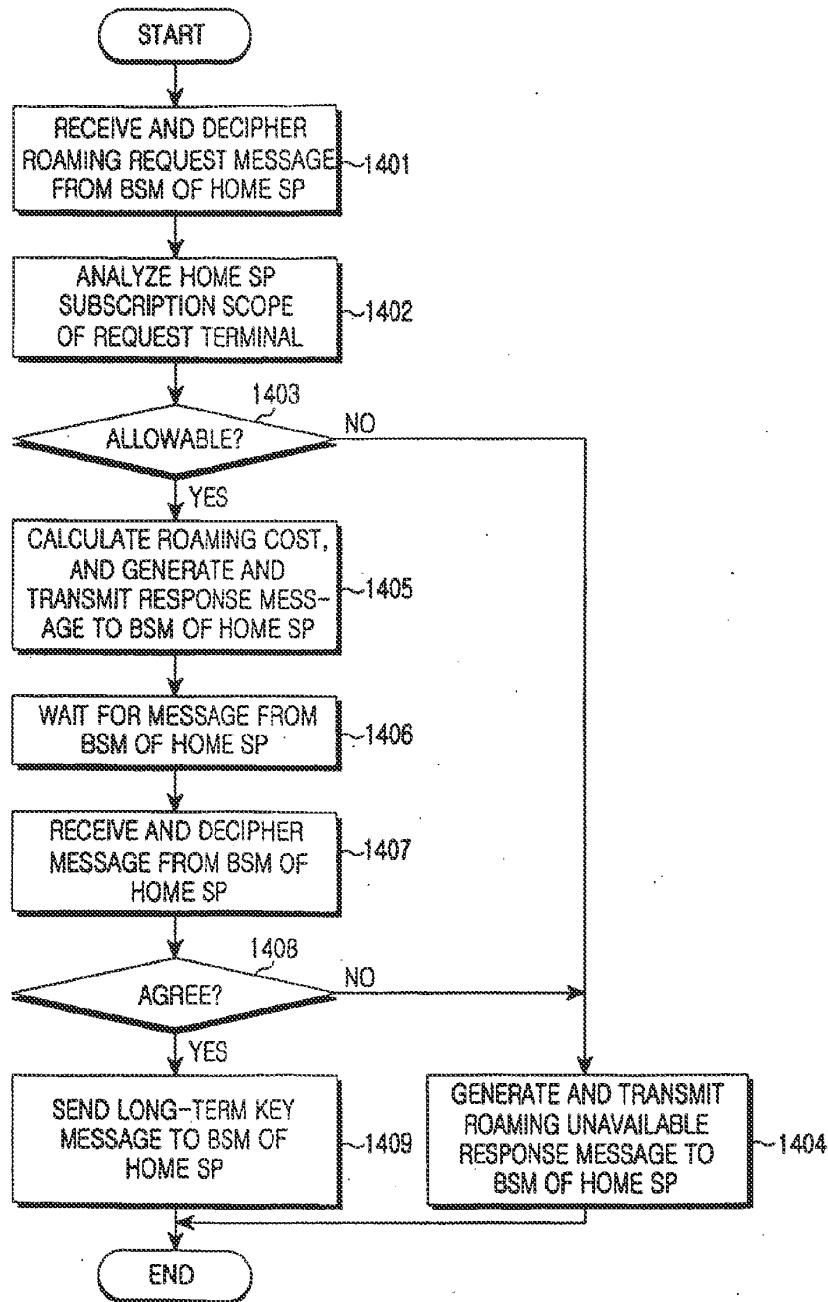


FIG.14

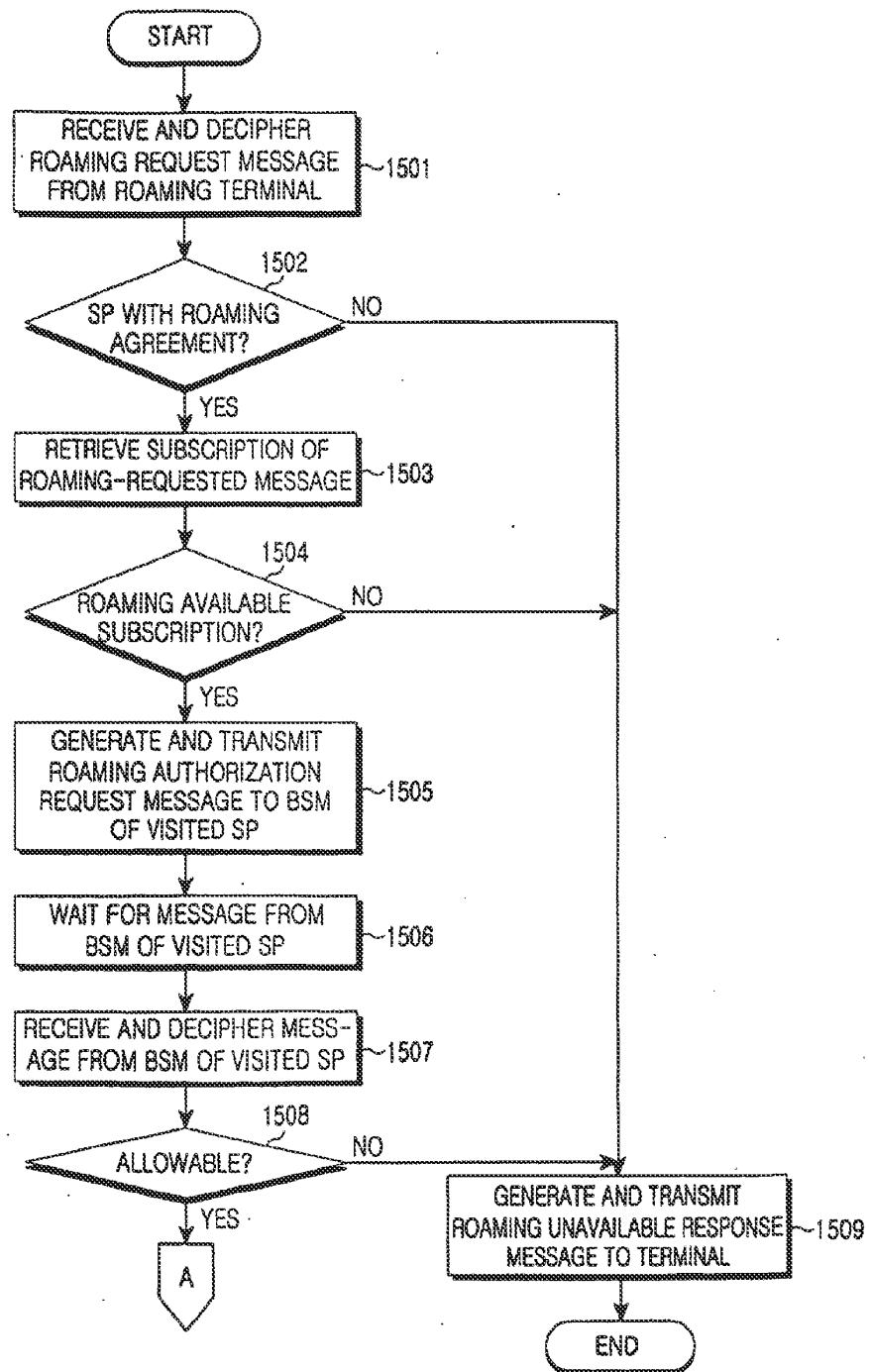


FIG.15A

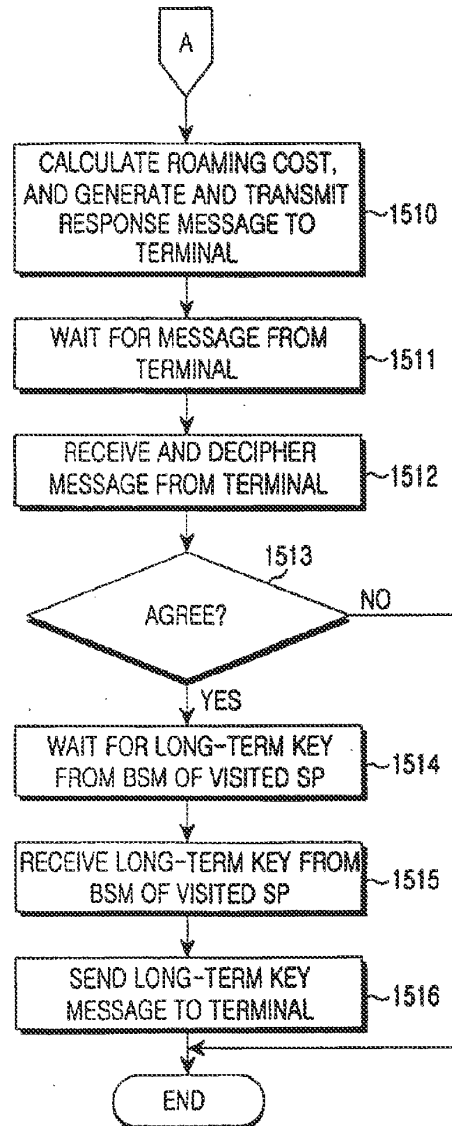


FIG.15B

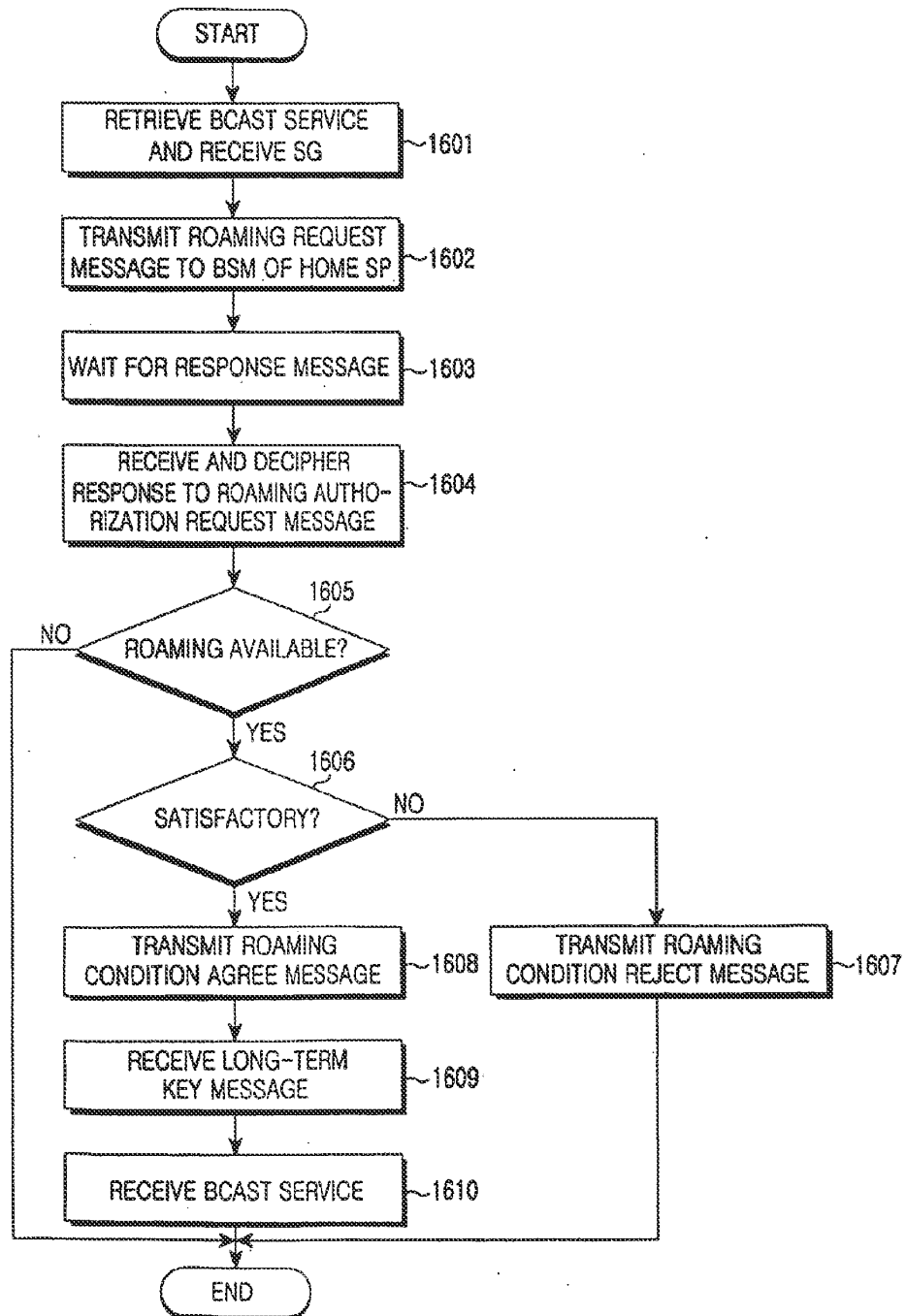


FIG. 16

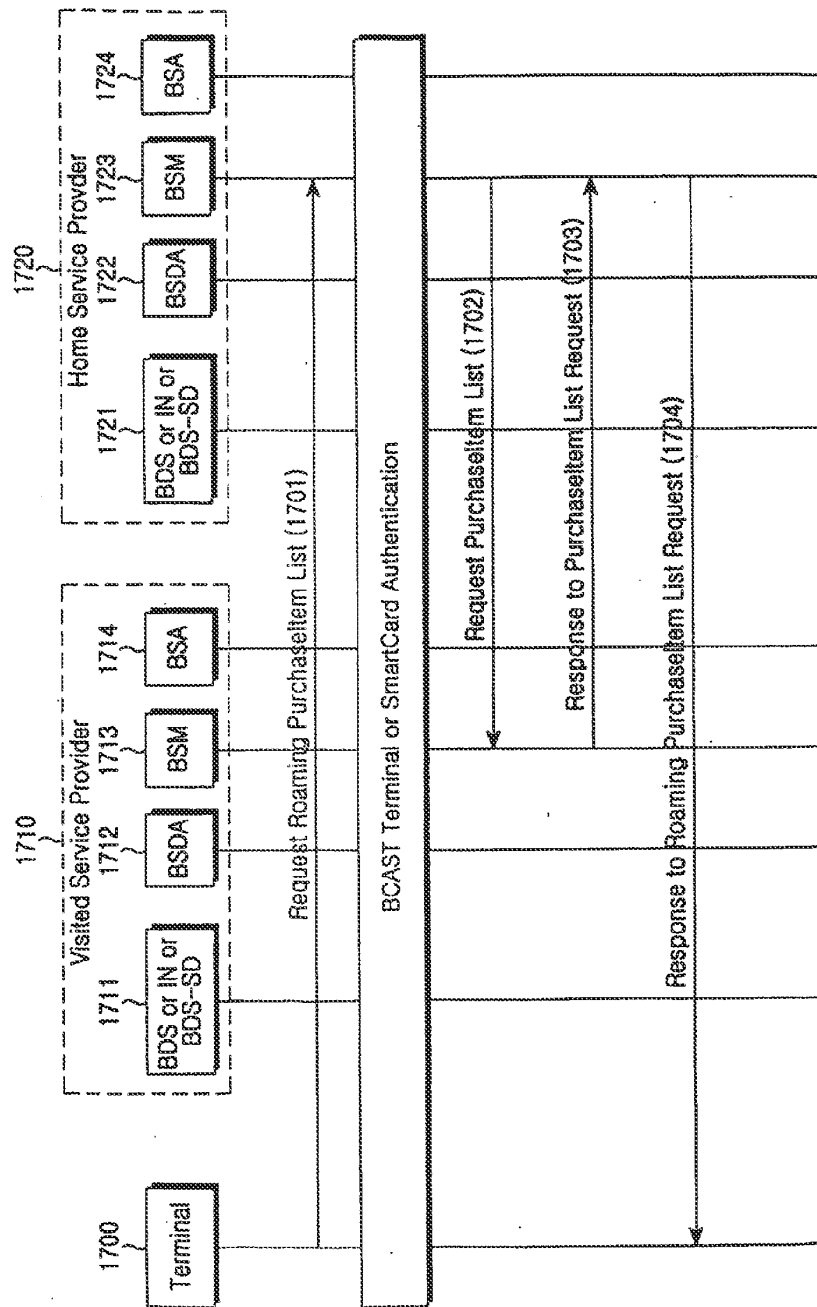


FIG.17

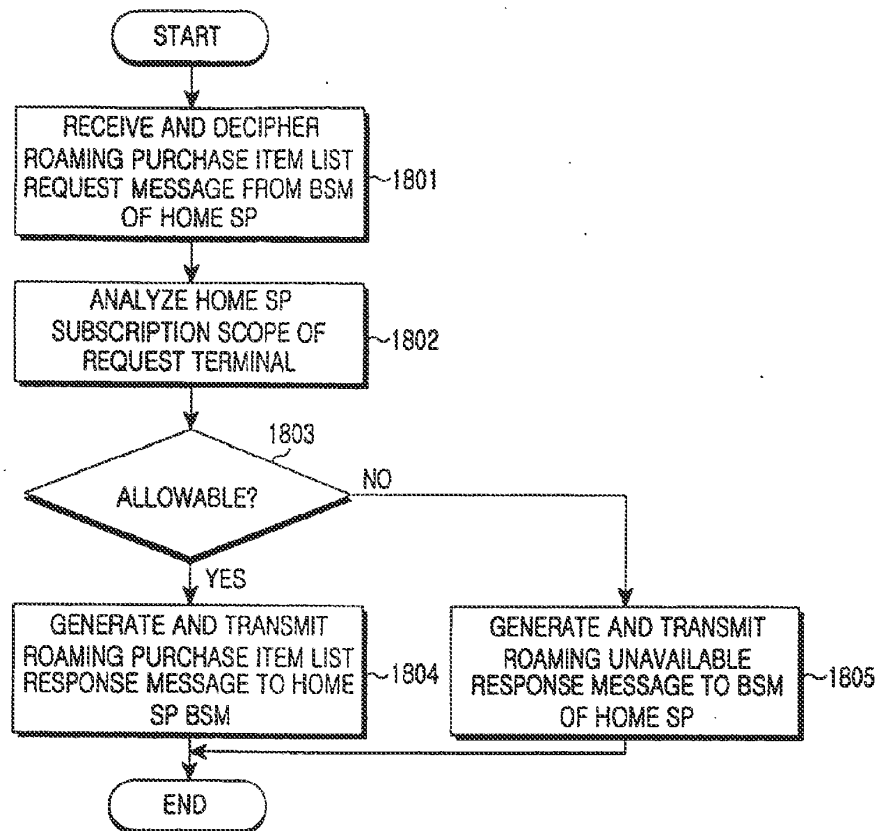


FIG.18

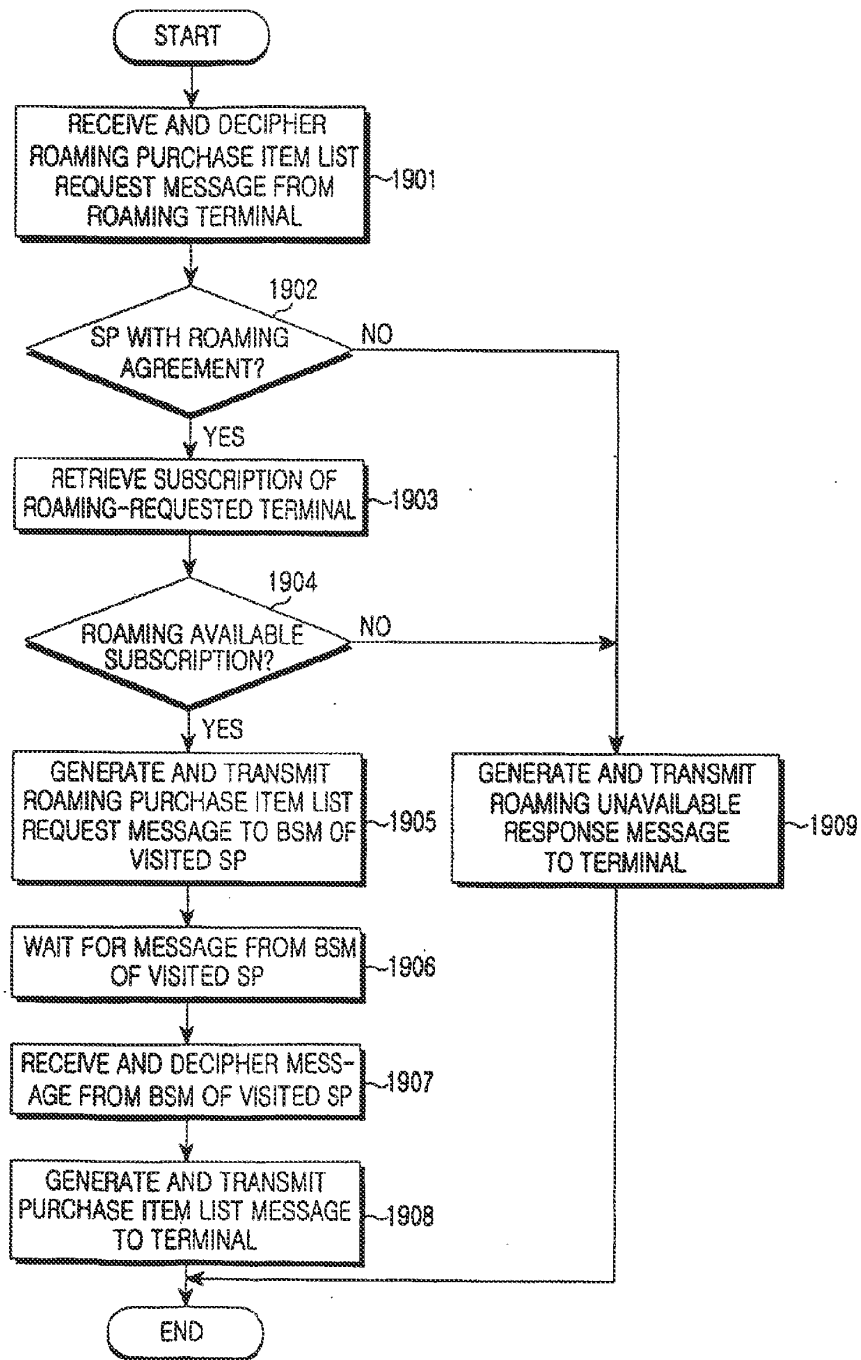


FIG.19

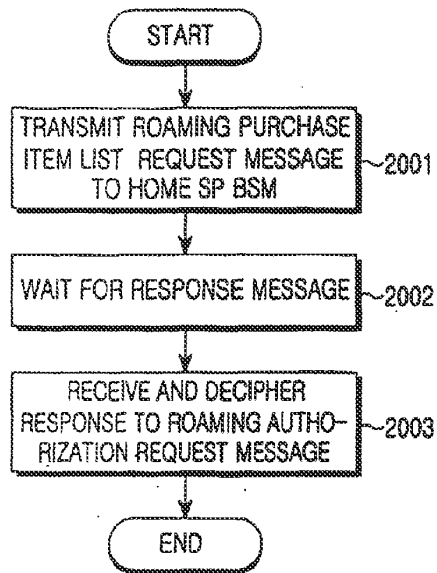


FIG.20

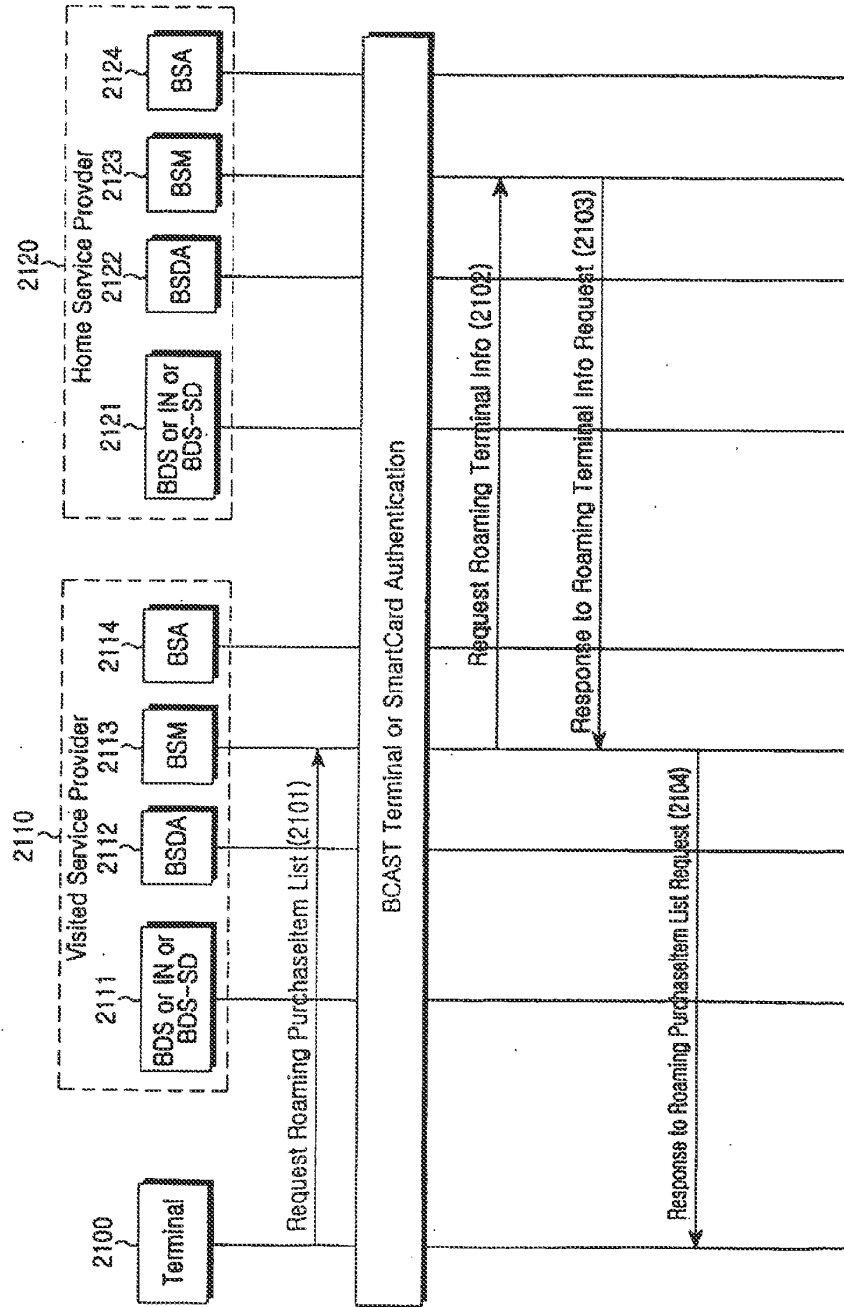


FIG. 21

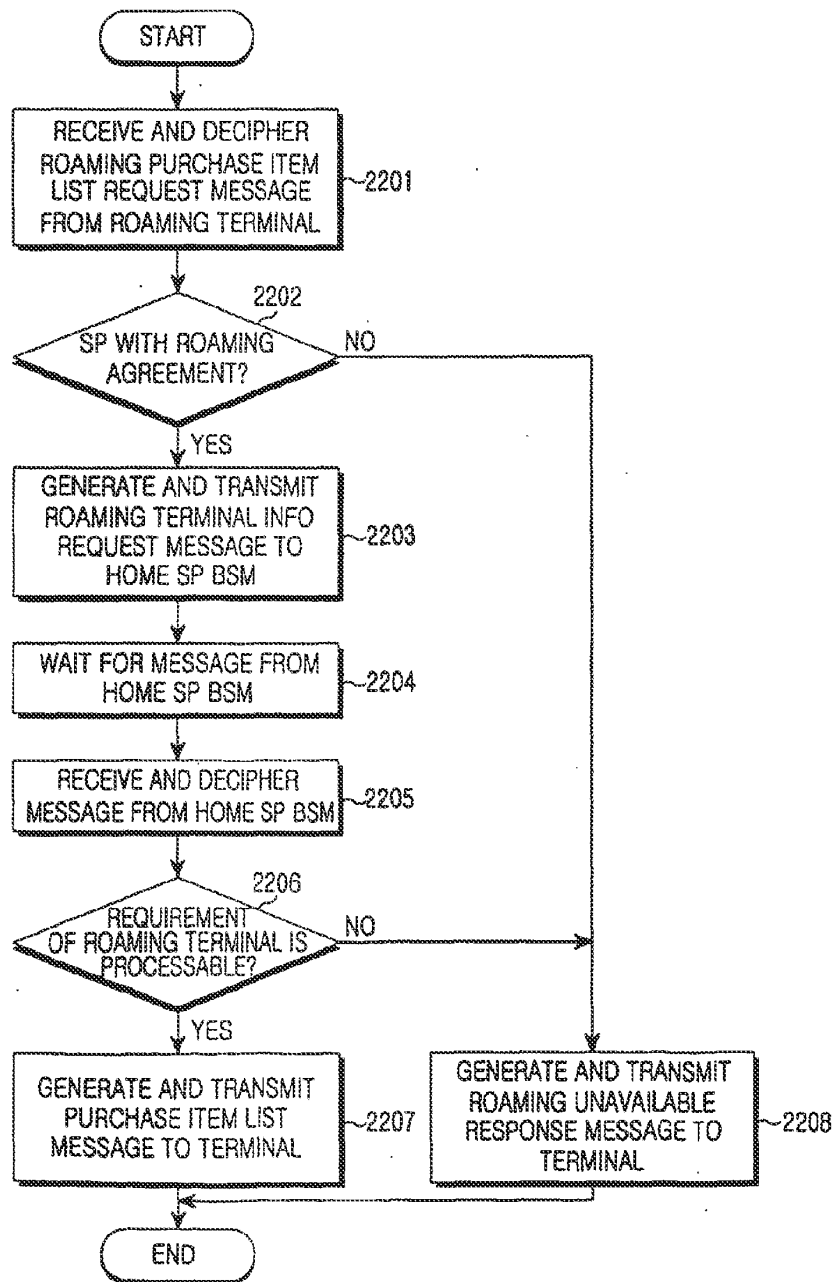


FIG.22

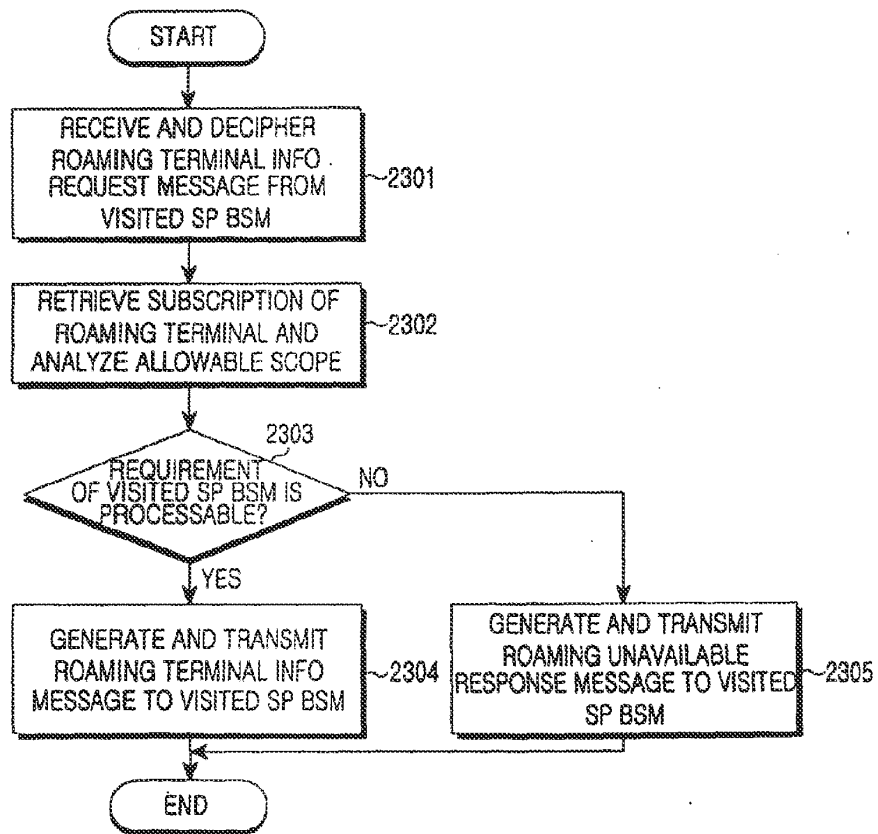


FIG.23

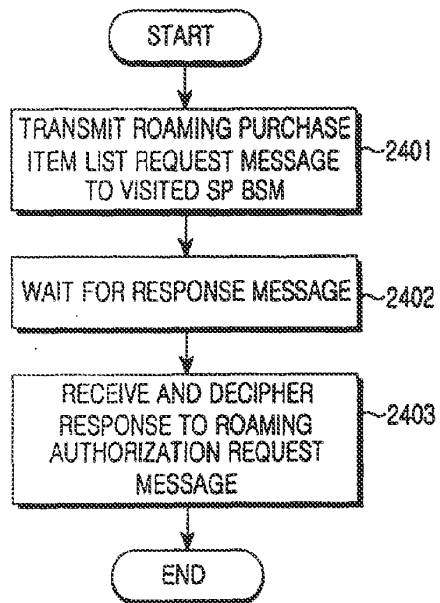


FIG.24



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 08 00 0788

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
P,X	WO 2006/014076 A (LG ELECTRONICS INC [KR]; HAN KYU-SUNG [KR]; SHIM DONG-HEE [KR]; SHON M) 9 February 2006 (2006-02-09) * paragraphs [0025], [0026] * * paragraphs [0048] - [0065] * * paragraphs [0068] - [0073] * * figures 1,6 *	5-7	INV. H04L29/06
Y	EP 1 538 861 A2 (SAMSUNG ELECTRONICS CO LTD [KR]) 8 June 2005 (2005-06-08) * paragraphs [0005], [0012] - [0020] * * paragraphs [0031] - [0038] * * figures 4,6,7 *	1-12	
Y	GB 2 406 754 A (NOKIA CORP [FI]) 6 April 2005 (2005-04-06) * abstract * * page 18, line 27 - page 21, line 9 * * figures 4,6,7 *	1-12	
			TECHNICAL FIELDS SEARCHED (IPC)
			H04L
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 27 February 2006	Examiner Bengi, Kemal
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03 02 (P04001)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 08 00 0788

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-02-2008

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 2006014076	A	09-02-2006	EP 1774718 A1	18-04-2007
EP 1538861	A2	08-06-2005	CN 1674711 A	28-09-2005
			KR 20050053172 A	08-06-2005
			US 2005130660 A1	16-06-2005
GB 2406754	A	06-04-2005	CN 1860707 A	08-11-2006
			EP 1687919 A1	09-08-2006
			WO 2005034396 A1	14-04-2005
			KR 20060060048 A	02-06-2006
			US 2006262751 A1	23-11-2006

EPO FORM P448

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- KR P200594675 [0058]



ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/577,237	11/22/2023 06:02:22 PM Z ET	RALEP007C11C3C2C3C2C1C1C1

Title of Invention

Automated Device Provisioning and Activation

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	5850	FILED BY	Evan Gunderman
PATENT CENTER #	63363736	FILING DATE	01/17/2022
CUSTOMER #	106963	FIRST NAMED INVENTOR	Gregory G. Raleigh
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Michael Farjami

Documents

TOTAL DOCUMENTS: 22

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
RALEP007C11C3C2C3C2C1 C1C1_IDS_Nov_22_23.pdf	6	Information Disclosure Statement (IDS) Form (SB08)	1233 KB
Warning: This is not a USPTO supplied IDS fillable form. Data in the form cannot be automatically loaded to other USPTO systems.			
Foreign_References.pdf	129	Foreign Reference	4504 KB
Exhibit 1010 Security Engineering.pdf	109	Non Patent Literature	19138 KB
Exhibit 1015 Internet Archive of CryptoGraf.pdf	1	Non Patent Literature	965 KB

Exhibit 1016 National Institute of Standards and Technology glossary of terms.pdf	2	Non Patent Literature	747 KB
Exhibit 1019 Headwater Infringement Contentions Exhibit B.pdf	104	Non Patent Literature	7140 KB
Exhibit 1004 Complaint Headwater Research LLC v. Samsung Electron-ics Co. Ltd. et al.pdf	25	Non Patent Literature	7768 KB
IPR2024-00003 Petition for Inter Partes Review.pdf	118	Non Patent Literature	12852 KB
IPR2024-00010 Petition for Inter Partes Review.pdf	113	Non Patent Literature	3829 KB
Exhibit 1004 3GPP TS-23.140 .pdf	218	Non Patent Literature	9538 KB
Open Mobile Alliance Multimedia Messaging Service Architecture Overview specification.pdf	26	Non Patent Literature	4509 KB
Exhibit 1011 Open Mobile Alliance OMA-ERELD-MMS-v1_2-20030923-C.pdf	16	Non Patent Literature	1683 KB
Exhibit 1013 Technical Specification Group Services and System Aspects TSGS0167.pdf	21	Non Patent Literature	2620 KB
Exhibit 1027 IETF RFC 793 Transmission Control Protocol.pdf	81	Non Patent Literature	6054 KB

Exhibit 1028 The TLS Protocol Version v 1.0.pdf	80	Non Patent Literature	18383 KB
Exhibit 1030 Needham Using Encryption for Authentication in Large Networks of Computers.pdf	7	Non Patent Literature	675 KB
Exhibit 1031 Schroeder A Hardware Architecture for Implementing Protection Rings.pdf	14	Non Patent Literature	1333 KB
Exhibit 1032 Saltzer The Protection of Information in Computer Systems.pdf	31	Non Patent Literature	12704 KB
Exhibit 1033 Li Symbian OS platform security model.pdf	15	Non Patent Literature	1542 KB
Exhibit 1034 Zimmermann Pretty Good Privacy RSA Public Key Cryptography for the Masses.pdf	35	Non Patent Literature	1462 KB
Exhibit 1035 Ramsdell SMIME Version 3 Message Specification.pdf	32	Non Patent Literature	18019 KB
Exhibit 1036 Mostafa Transporting data between wireless applications using a messaging system.pdf	12	Non Patent Literature	885 KB

Digest

DOCUMENT

MESSAGE DIGEST(SHA-512)

RALEP007C11C3C2C3C2C1C 1C1_IDS_Nov_22_23.pdf	60E2B098333B666E41FD10E46BF24E3DE71AA32B2605A97193 876F232DCA83BC381A95452524D23BC3CC8FCD3439F248BEB 5B2741B8F122C6F3594E7678E2B0E
Foreign_References.pdf	949BD8A4B9E7D52221471B2C7A5DC4F3D12EAABD891A71F1 2FACB0B312807C8B5E017D1E1DB2A3A024A69D0E6CEC5A65 EAA9D705977C3458F7481CBEFA304F1C
Exhibit 1010 Security Engineering.pdf	6DB7B2785C3E7241D270B24B9DA77234CAF AA052ABB8DAD4 FE23FB3A00A0F5853661B890C7A8CB1E720A5A087C9BBD1C4 9E5643AD8796937AC396CF69500E3F6
Exhibit 1015 Internet Archive of CryptoGraf.pdf	A288A47B8FD9DC751899CCC63BE57A2B28A9FDC7D7FFA7D8 E370A478FC319354C1C07D689FE980485D462716DE11806B80 D75C8A834BC464AA32BCED1C37B75E
Exhibit 1016 National Institute of Standards and Technology glossary of terms.pdf	173108C0FC472DC4BC62D5586B6861FB3860CB2FB5B14DFC4 0ED051D4AB3EF9E5E59F5211D4E3D6EDB68F548B0D35874D AFE50C7CC5A2A476ECC509910B3C7D3
Exhibit 1019 Headwater Infringement Contentions Exhibit B .pdf	1D6A4C87F450882735C27182D3B8F5E023D9CB59BA67B5EC4 0512A58D5EBE7CBB828B9F46E858F5784741A82EDA09252F25 07F324009A2B06C1DE9A13B9B0D8E
Exhibit 1004 Complaint Headwater Research LLC v. Samsung Electron-ics Co. Ltd. et al.pdf	0F5AA739545013EE77C83F75012FEBE0FEA77C47CACA7FBA2 37F811E2412F37EC324A1E1D21A04434FDE1714AED153C226 D4AC590D1B67B354EB8BCACED04964
IPR2024-00003 Petition for Inter Partes Review.pdf	52F7F403D2D86FF3706989F611602ABB9F54400DAEDCDACC D990240A04739BA110DDB49758FE21F5C9C1D3162C471B424 D455BD505736858E71A5DEC51BA2848
IPR2024-00010 Petition for Inter Partes Review.pdf	FD36603DF1EE4F40B3A3500796B4823FD0C7BACD666565B92 F48D808B1E9A4642FEE34467E50F46396C13BE4F530F939927 BFC532206BC135D19BBE22D0D549F
Exhibit 1004 3GPP TS-23.140 .pdf	DD57EC0D5B46FC976DB6A3040FF937D7C6F4EBD6142461164 331DD280B8DB3A6F468C70F19F03DB741E7F4761A7A3DA822 C496A61A5B5586A825049D5CC834AC

Open Mobile Alliance Multimedia Messaging Service Architecture Overview specification.pdf	06D23326935D7D4639B012C7425E6200E962097BF57832280B6 823AB9541253AF7782922D0998C3932A0BF787D8944E0062B2 E58630A7606758B1612E1974FA9
Exhibit 1011 Open Mobile Alliance OMA-ERELD-MMS- v1_2-20030923-C.pdf	3E73E43248494FA73A847415338AEB1E1F5953B9EB17A765FC 13A732CC3CDC9A1DC59E8122F20DF993B1CC1B6464835EF0 299730922556056B130C537146C800
Exhibit 1013 Technical Specification Group Services and System Aspects TSGS0167.pdf	117CC8984E281659473E691FC708CA28B334F1CB3F2879495E 1F9CC61A0ED3556C51E49F6BF541D749F740A97ED163E31B7 72837B285C27CBCA3084129B007B1
Exhibit 1027 IETF RFC 793 Transmission Control Protocol.pdf	D6B1BD244F644BD714CF2FD76464C0B05A2C45B4B102F997C F4A2F3B1390838EC27848165DCF3A87FF77FDEF51984D44F80 CCD8029C97BF93FD0D65AC2824000
Exhibit 1028 The TLS Protocol Version v 1.0.pdf	F7EE338551E6FA865332ACDE1FAD45CAEDC534E4DBEF311A 5FF883E11158284B14891814DE52D0D3BFB7FD8BCCF1E487B B1A358850DCAC1DB5AD6C71E8B5A0E0
Exhibit 1030 Needham Using Encryption for Authentication in Large Networks of Computers.pdf	C01B88436A6FA08C77D6D6B5EB5C4CAE5DE16FEBF9002C5E 96DFBFF198F068A3ECF2AC6279C2F2E56290CFEDE710C6000 FF2B7D37302C40254DAF06D8FE86C92
Exhibit 1031 Schroeder A Hardware Architecture for Imple-menting Protection Rings.pdf	6EEF98C1AA557DA4DEABE71B605A8E024DE4F01C9DB660F5 B84E8C7E5DC7A1E087B4CF4B5E4EB3C3328FFCA865AAEA68 4905286D99D4C9CCE6A26239225CFB84
Exhibit 1032 Saltzer The Protection of Information in Computer Systems.pdf	0332236F7C3BEAD80FEE48BEB293E44D13C1892AB1E8D710B 09D8D46761ABD352CA92F49145EF13282AAD96107572D78EB 1265BA09343EC52CC59CFEDB3EC93A
Exhibit 1033 Li Symbian OS platform security model.pdf	A3818EA1CB29087002A9B7DCBE51EF1F77A1104A76C309421 027AF8AEC5C86DFD0B8AAF9D5FB71128CF67B07B4EC9DCB4 47312E4B3C2B677087EA10F57F044A4
Exhibit 1034 Zimmermann	4BAEA459BB422769096C2EB08F99E0D626EEF269B3F11799A

Pretty Good Privacy RSA Public Key Cryptography for the Masses.pdf	2ECAFB0B44C060A1CC785F926B02C118649BE3D2CFFE41856 87DEB5B0066BE514FACEC1329B2BF5
Exhibit 1035 Ramsdell SMIME Version 3 Message Specification.pdf	0A11F86DE35C549A40689CFA2A8E8AC82F17ECF699C8F1CC 9DAD2F756F59FD8A0FDC15522DDF24CAE1B07986D97F4EF0 B5C169A85A9F3041452D993236380ECF
Exhibit 1036 Mostafa Transporting data between wireless applications using a messaging system.pdf	2F1A717EFE2D951B2F1EE5B9E89B8C8A490973C9CAF342D1F 8CDA7954A1EB649FBACCD8B15879704C4E082FEA4B4EE13B 75C42DDD202E304DB8304A76F66B103

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	3687		
	Examiner Name	Unknown		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7082615		2006-07-25	Ellison	
	2	8041816		2011-10-18	Ozaki	
	3	7925717		2011-04-12	Chou	
	4	7509487		2009-03-24	Lu	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20070011736		2007-01-11	Kalibjian	
	2	20090240807		2009-09-24	Munson	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		3687	
	Examiner Name		Unknown	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	3	20090282256		2009-11-12	Rakic	
	4	20040122907		2004-06-24	Chou	
	5	20040105431		2004-06-03	Monjas-Llorente	
	6	20070214245		2007-09-13	Hämäläinen	
	7	20050207379		2005-09-22	Shen	
	8	20060190720		2006-08-24	Ozaki	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2006077283	WO			Houghton		☐
	2	2008048075	WO			Lee		☐
	3	1853044	EP			Shenfield		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	3687	
	Examiner Name	Unknown	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Security Engineering "A Guide to Building Dependable Distributed Systems," second edition, 2005 by Ross J. Anderson	☐
	2	Internet Archive of CryptoGraf, accessed Sep. 20, 2023, available at https://web.archive.org/web/20070210050616/http://www.cryptograf.com/	☐
	3	National Institute of Standards and Technology (NIST) glossary of terms, accessed Sep. 20, 2023, available at https://csrc.nist.gov/glossary/term/aaa	☐
	4	Headwater Infringement Contentions for U.S. Patent No. 9,198,117 vis-a-vis Samsung's mobile electronic devices	☐
	5	Complaint, Headwater Research LLC v. Samsung Electronics Co., Ltd. et al., 2:23-cv-00103, E.D. Tex., March 10, 2023	☐
	6	IPR2024-00003; Petition for Inter Partes Review of United States Patent No. 9,198,117, filed on November 17, 2023	☐
	7	IPR2024-00010; Petition for Inter Partes Review of United States Patent No. 9,615,192, filed on November 17, 2023	☐
	8	3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2 ("TS-23.140")	☐
	9	Open Mobile Alliance; Multimedia Messaging Service Architecture Overview (MMSARCH) specification, available at https://www.openmobilealliance.org/release/MMS/V1_1-20040715-A/OMA-WAP-MMS-ARCHV1_1-20040715-A.pdf	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	3687
	Examiner Name	Unknown
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

10	Open Mobile Alliance; OMA-ERELED-MMS-v1_2-20030923-C, "Enabler Release Definition for MMS Version 1.2," available at https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMAERELED-MMS-V1_2-20030923-C.pdf	☐
11	Technical Specification Group Services and System Aspects Meeting #19, TSGS#19(03)0167, European Telecommunications Standards Institute February 2003 (available at https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_19/Docs/PDF/SP-030167.pdf)	☐
12	IETF RFC 793, Transmission Control Protocol (Sept. 1981) (available at https://www.ietf.org/rfc/rfc793.txt)	☐
13	The TLS Protocol Version v 1.0 (Jan. 1999) (available at https://datatracker.ietf.org/doc/html/rfc2246)	☐
14	Needham et al., "Using Encryption for Authentication in Large Networks of Computers" (ACM, Vol. 21, No. 12, Dec. 1978)	☐
15	Schroeder et al., "A Hardware Architecture for Implementing Protection Rings" (ACM, Vol. 15, No. 3, Mar. 1972)	☐
16	Saltzer et al., "The Protection of Information in Computer Systems" (IEEE Proceedings, Vol. 63, No. 9, Sept. 1975)	☐
17	Li et al., "Symbian OS platform security model," available at https://www.usenix.org/system/files/login/articles/73507-li.pdf (Login Magazine, Aug. 2010)	☐
18	Philip Zimmermann, "Pretty Good Privacy: RSA Public Key Cryptography for the Masses" PGP User's Guide. Version 1.0, June 1991), available at https://www.techinsider.org/free-software/research/acrobat/910605.pdf	☐
19	B. Ramsdell, S/MIME Version 3 Message Specification, IETF RFC 2633, June 1999, available at https://datatracker.ietf.org/doc/html/rfc2633	☐
20	Mostafa, "Transporting data between wireless applications using a messaging system—MMS" (Wireless Comms. and Mobile Computing, July 7, 2006)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	3687
	Examiner Name	Unknown
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

If you wish to add additional non-patent literature document citation information please click the Add button			
EXAMINER SIGNATURE			
Examiner Signature		Date Considered	
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			
<small> ¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached. </small>			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	3687
	Examiner Name	Unknown
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2023-11-22
Name/Print	Farshad Farjami	Registration Number	41014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
27 July 2006 (27.07.2006)

PCT

(10) International Publication Number
WO 2006/077283 A1

(51) International Patent Classification:
H04L 12/56 (2006.01) *H04Q 7/22* (2006.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/FI2006/050032

(22) International Filing Date: 19 January 2006 (19.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20050067 20 January 2005 (20.01.2005) FI

(71) Applicant (for all designated States except US): **STREAM MOBILE OY** [FI/FI]; Tammasaarenlaituri 3, FI-00180 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HOUGHTON, Paul** [US/FI]; Helmitauluntie 13b, FI-02770 Espoo (FI).
REHTIJÄRVI, Pekka [FI/FI]; Itälahdenkatu 13 A 32, FI-00210 Helsinki (FI).

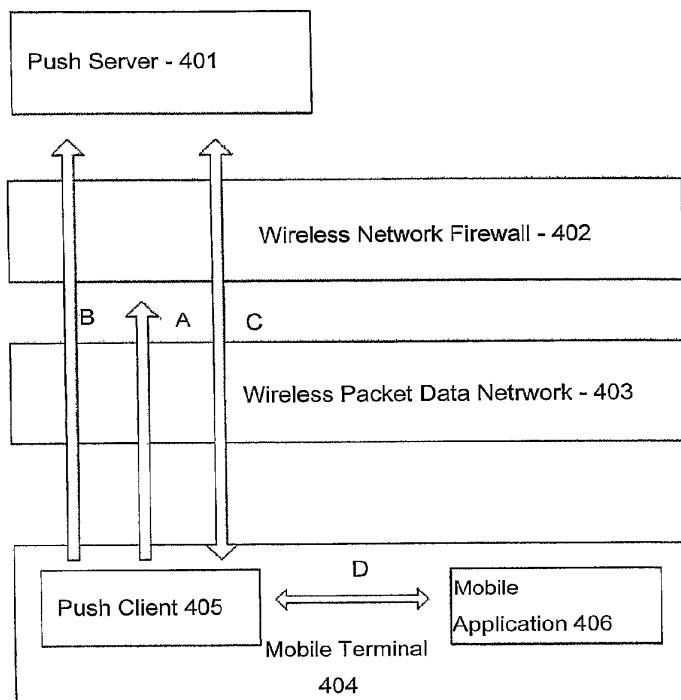
(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O. Box 148, FI-00121 Helsinki (FI).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PUSH MESSAGING COMMANDED METHODS AND DEVICES



(57) Abstract: A server outside a wireless network security entity is adapted to push messages to a mobile terminal located in the wireless network and thereby cause programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message thereby presenting a new application view to the user of the mobile terminal. The mobile terminal is provided with means, such as software, which initiates and maintains contact with the server using Internet technologies. This mobile-initiated permanent connection allows the server to pass or push messages from outside the operator's firewall to the mobile terminal at any time.

WO 2006/077283 A1



Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- of inventorship (Rule 4.17(iv))

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- with international search report

Title of the invention

Push Messaging Commanded Methods and Devices

Field of the invention

The invention relates to techniques for launching applications on a mobile terminal.

Description of the Related Art

The Internet is a collection of networks which exchange messages using IP protocol (Internet Protocol) and associated protocols which run on top of IP such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Gateways between IP networks automatically route and transmit information over primarily the IP4 and IP6 protocols between two or more end points on any of the connected fixed and mobile networks. Each of these networks may also include or run on top of other network transport protocols such as ATM (Asynchronous Transfer Mode) or a wireless protocol which in turn carry the IP packets over that section of the Internet.

Currently, the most common method of starting applications on a mobile terminal is to manually launch them by clicking on an icon or selecting a menu item. If the application, dynamically loaded program module or user interface feature is already launched, these applications must also be manually commanded by the user to change state to display newly available information provided by a telecommunications network. Some applications are also launched automatically when the terminal is started. This automatic start includes both applications that were installed on the phone before delivery to the customer including the basic terminal operating system software and programs installed by service providers and users and which by various means ask the terminal software to start them automatically after the terminal is powered up.

Remote launch to a known state as specified in a network command of programs on mobile terminals is supported in various telecommunications standards. Voice Over IP (VoIP) and other multimedia sessions can be started remotely using Session Initiation Protocol (SIP). Wireless Application Protocol Push (WAP Push) is another standard for launching programs on mobile terminals based on remote events. Java Mobile Information Device Profile (MIDP) and various native mobile terminal operating systems also support remote application launch based on receipt of a text message (Short Message Service,

SMS) or incoming Internet (IP) packet of information to a designated communications port number. However it is important to note from an economics and practical service deployment standpoint that each of these technologies either requires payment to the mobile network operator for sending an SMS or privileged access to the mobile phone from inside the operator's firewall in order for IP data to actually reach the phone.

Mobile phones and similar mobile communication devices were originally not permanently connected to the Internet. Instead, for the transmission and display of visual information they have relied on different telecommunications standards and proprietary communication systems such as SMS (Short Message Service, also known as text messaging) and MMS (Multimedia Message Service), which were built into mobile terminals.

Various techniques have been proposed for remotely commanding applications on a mobile terminal using push technologies:

US20020183051 relates to remote application management of a wireless device.

US20030208602 relates to pushing data in an internet protocol network environment.

US20010020255 relates to remote control and interaction with a mobile run time environment component.

US6687743 relates to client server communications for a mobile computing device.

US6779019 relates pushing information from a host to a mobile data communications device.

US6701378 relates pushing information from a host to a mobile data communications device.

US6463464 relates pushing information from a host to a mobile data communications device.

US6463463 relates pushing information from a host to a mobile data communications device.

US6389457 relates pushing information from a host to a mobile data communication device.

US2004122907 relates to secure interaction between a mobile client device and an enterprise application in a communication system.

WO0195695 discloses a system for wireless push and pull based services.

US2002187775 discloses a WAP service personalization, management and billing object oriented platform.

US2003106022 relates to outputting dynamic local content on mobile terminals.

US2004185834 discloses a method for enabling IP push capability to wireless devices on a wireless network.

US2002174184 shows a mailbox access mechanism using SMS push and WAP technologies on mobile terminals.

WO02077842 shows a push method for delivering data to mobile device.

Wireless Application Protocol Forum, Ltd., "Wireless Application Environment Specification, Version 2.0", Version 7-Feb-2002, 2002.

www.wapforum.org.

Sun Microsystems, Ltd., "The MIDP 2.0 Push Registry", Network and Timer MIDlet activation. developers.sun.com/techtopics/mobility/midp/articles.

Nokia, Ltd., "SIP Session Initiation Protocol", Forum Nokia 2005. www.forum.nokia.com/main/0,6566,1_44,00.html.

Nokia, Ltd., "SIP Frequently Asked Questions", Forum Nokia 2004. SIP_FAQ_v1_0_en.

RFC 3261, "SIP: Session Initiation Protocol", 2002. www.faqs.org/rfcs/rfc3261.html.

Push technology is characterized by the server proactively sending documents or information to a client or user. E-mail (Electronic mail) is actually a special kind of push technology that has been prevalent for a long time. The first and most common general category of mobile content push technologies is SMS (Short Message Service) based technologies. SMS and MMS (Multi-media Messaging Service) are the most common forms of "push" messaging in the mobile industry. These store and forward messaging systems run by mobile telecommunications operators push all or part of the data to the mobile terminal over closed telecommunications signaling networks such as SS7 (Signaling System Seven). These signaling networks are closed; they are not part of the Internet. Each operator controls and encrypts this traffic, charging high prices for their use and limiting their use and usefulness.

FIG 1 shows a generic implementation known in the art for pushing launch and operational commands to applications on mobile terminals. Email, MMS, WAP (Wireless Application Protocol) pages, and custom application

data are delivered through existing telecommunications infrastructure to a mobile terminal using SMS as the push messenger medium. First, push server software 101 delivers the notification to an SMS Gateway 102, as illustrated by the arrow A. The SMS Gateway puts the actual SMS push message in either readable text or compressed binary format into the telecommunications signaling network 103, usually SS7, which delivers it in a store and forward fashion often involving several intermediate steps to the mobile terminal 104, as illustrated by the arrow B. The mobile terminal standard software 105 decodes header information in the SMS and based on the fields in this binary SMS header not visible to end users, delivers this as a normal SMS, an MMS, WAP pages or a custom application command action (C) to the indicated mobile application 106, launching the application if necessary. These custom application launches by SMS require the application to first register itself with the mobile terminal in order to receive SMS push message command events.

Besides a high price per message, SMS messages cost different amounts depending on where the sender and receiver are located. In some countries the sender pays for the message, in other countries the receiver pays. Computers called Short Message Service Center (SMS-C) nodes and owned and managed by each mobile operator deliver SMS messages. In many cases, if the sender and receiver are on different continents the operators do not even offer message delivery. Two operators must negotiate, sign and implement a legal contract known as an interconnect agreement before messages flow between SMS-Cs and thus between mobile terminals on different operator networks. Since not all operators have such contracts with all other operators, this limited connectivity also means that commanding mobile applications based on any SMS technologies can not be delivered on a global basis. For example an SMS-based remote application command server run from a European telecommunications operator will face the practical limits of incomplete operator interconnect agreements when pushing application commands to their North American and Asian customers. Also, because of the billing models in different countries are also variable, high costs and delays when roaming, it is difficult to develop reliable global application command using SMS-technologies. For example, such SMS delivery arrangements to all operators within one country or in multiple countries usually rely on expensive arrangements with middlemen or brokers that route computer-originated mes-

sages to phones in many locations. Even the best of these such middlemen still do not offer global coverage to all countries.

A newer telephone company standards-based method to delivery content and command applications which have not been explicitly requested by the user of a mobile terminal is WAP Push. WAP Push technology relies on an SMS to start the message delivery process. Both SMS and WAP Push using SMS can be used to command applications on the phone. Java applications on mobile terminals can also register themselves to be launched upon receipt of an SMS and then interpret the contents of the SMS as a type of launch command or launch content. But in all these cases operators continue to control the push medium and charge money for each push event. This operator control of content on mobile terminals is known in the industry as the "walled garden" approach.

SMS messaging standards include the ability to send binary messages to an application installed on the mobile terminal. Parameters in the message header and applications in the mobile terminal are matched by the mobile terminal at delivery time and the selected application receives the pushed SMS contents, starting the application if it is not already running. This is a standard software feature installed on the phone at time of manufacture as part of the mobile terminal's operating system.

The cost of using such an remote command capability is quite high- the cost of an SMS each time the program is commanded, thereby limiting the broad utility of this feature for all but a telecommunications operator supplying the service only to their own customers. These standard SMS-based telecommunications technologies for push application remote command are all thus limited by economics in both the frequency with which they can be used and the breadth of market which they can reach. Also due to the low speed of SMS delivery as a store-and-forward messaging system, it can take a long time for the application to launch to a known state based on a remote command thus making this unsuitable for use in any real time or time critical situations.

A further limitation of existing SMS remote command technologies is the inability to prioritize, select and deliver messages in different ways to a user based on their current situation, location and individual preferences. More important application command events may be buried behind several less important events causing critical items to be missed or confused. A user can not select with these SMS-technologies not to be notified, or to be notified in a

more polite manner, or to go ahead and start to a known state or change the visible operating state of the application without politely asking in some circumstances. And a user can not specify that they would like to only receive or receive a request for permission to execute a certain category of application command events during a given period of time.

A second general category of mobile push technologies is IP-based technologies. These include IP connections initiated from the server and IP connections initiated from the client. Server-initiated push connections are the most commonly described. These solutions require IP communication with software installed on the terminal and a server which has been notified of the IP address of this terminal. The server then, when a push event is desired, initiates a connection to the terminal and delivers information to it which software in the mobile terminal can then act upon, most commonly to notify the client of an incoming email message. For reasons described below, these push technologies are not generally used on mobile terminals but are more commonly used between one server and another as in the SMTP mail transport protocol when delivering email. Similar methods are also used for launching, commanding and communicating with applications on servers and in some cases on mobile terminals.

There are, however, difficulties with commanding applications on mobile terminals based on receipts of an IP packet when there is not an already established IP connection between a mobile application program module or feature and the command push server. In practice, mobile terminals are on sections of the Internet which are most commonly behind a firewall or gateway server device creating a controlled mobile network. This difference from the above-mentioned server-to-server push technologies is non-obvious when reading standards and results in many server-to-client and server-to-mobile-terminal push technologies which in practice do not work because of firewalls protecting the mobile terminal. Thus firewall and mobile gateway devices at the connection between the security-controlled mobile network and the more public Internet frequently restrict computing devices such as servers on the public Internet from directly contacting mobile terminals. Additionally, IP connection and security techniques, such as network address translation, firewalls and gateways, may hide the actual address of the mobile terminal further complicating direct connection from an Internet computing device. Further, the mobile

terminal may be unavailable at any given time making such messages undeliverable.

The public telecommunications operator, company, organization, or private individual setting up a mobile Internet space with one or more users uses the above-mentioned firewalls, security devices and gateways to protect the mobile terminals from hostile or unwanted contact common on the public Internet. They may also do so to reduce background traffic, protect their control over this space and thereby limit outside or undesired service providers through technical connection policies set in the firewall or gateway device. The result is, if a fixed or mobile computing device from outside the controlled mobile network tries to contact a mobile terminal inside the controlled mobile network, the connection is not permitted unless the organization or individual controlling the firewall or gateway server device makes an exception to their security policy and explicitly allows the connection. Instead, in standards-based mobile Internet telecommunications, an intermediary computer with privileged access from inside the firewall to the mobile terminals is used. These server computers such as a telecommunications operator SIP Server or WAP Gateway is used to control and deliver messages and store messages when the mobile terminal is unavailable and deliver them on the senders behalf, possibly later then the terminal becomes available, or to forward them to a different gateway device, for example if the user is roaming to a different controlled mobile network.

The most common solutions to accessing mobile terminals subject to this mobile network restriction are to either make an agreement with the public or private network operator removing the security restriction on a specific outside server contacting mobile terminals, or to move the server inside the controlled network. In the common case of a public mobile network operator, the state of the art and most common solution is to sell the server and associated software to the mobile operator so that they can provide the service to their customers. Both of these solutions require time, effort and often large financial commitments. And they must be done for each and every restricted mobile network and operator in a given market to achieve universal access to a service requiring server-initiated IP push. Achieving such universal penetrations on all operators in all markets is not practical. However for those operators with whom such a relationship has been established, mobile application launch and command with standard IP technologies is thus possible.

Client-initiated mobile IP connections are less common in mobile terminals. These are also not part of state of the art mobile application command telecommunications standards. Client-initiated IP connections involve installing more complex software on each mobile terminal and having these devices initiate contact to a server on the public Internet. These connections generally operate in a polling or "content pull" manner, connecting intermittently to the server to ask if any new information is available. Mobile email is a common example of this approach for content download. While the result appears to be push to the end user when they are notified several minutes later of the incoming email, they were not notified immediately by the server when the message is available as in true push technologies. The network settings of the mobile terminal may also need to be adjusted to permit this since Internet access through default gateway devices may not permit this type of connection.

FIG 2 shows a generic implementation known in the art for pushing launch and operational commands to applications on mobile terminals using Internet technologies. Symbian, Linux, Microsoft and other mobile IP terminal operating system software all include application launch capabilities based on this socket-based triggering mechanism. Each mobile application 205 has a fixed IP port number such as TCP/IP or UDP/IP port numbers. When a remote program such as a push server 202 sitting inside the operator's firewall 201 and with permission to contact ports on the mobile terminal 203 sends an IP packet to the terminal (A), the IP terminal software 204 routes the packet with its commands or application-specific data to the mobile application 205 (B), launching the application if it is not already running. Java applications sitting on top of the lower levels of IP terminal software can be similarly launched based on Java MIDP 2.0 and later "push registry" settings.

FIG 3 shows the same steps A and B shown in FIG 2, however the push server 301 may be located outside the firewall 302 because the wireless network firewall has been configured by the mobile network operator to allow communications from that particular push server. This allows IP traffic to flow from the push server 301 to the IP terminal 303 and be internally routed 304 to the mobile application 305.

The important point to note in the standard methods shown in both FIG 2 and FIG 3 is that the permission of the wireless network operator is required to either locate a push server within their firewall or open a firewall hole to a given push server. This permission is in practice expensive for an arbitrary

push server to achieve with a given operator. It is virtually impossible to achieve with all mobile network operators in all markets. A viable market alternative to the state of the art methods shown in FIGURES 1, 2 and 3 for the mobile terminal and push server to initiate and maintain contact for push application launch and configuration commands without explicit arrangements with each mobile network operator is thus needed and described in the invention below.

Once such an IP connection is established between the server and one or more mobile terminals, the connection can be used to transfer messages to the mobile terminal. The most interesting such messages for the present invention are event trigger messages to launch or command a mobile application. Other interesting uses include the sending of data files, new applications and applications updates to replace or improve installed applications. These messages, while simply inexpensive IP traffic can if sufficient in number result in significant costs or the user perception of their incurring significant data traffic costs. For this reason it is also desirable to route such information including application updates, bug fixes, additional features, additional application data including multimedia, vector graphics, text and executable code through the lowest cost available network connection. Further it is desirable but not generally possible to automatically do so only during those times that a lower cost network connection is available as through the presence of a broadband wireless access device.

Numerous mobile applications such as games and productivity software are now included with new mobile terminals. They can be used to perform an endless variety of tasks, some of which involve interaction with elements outside the mobile terminal, for example on desktop computers, servers and other mobile terminals which are also connected to the Internet. The process of a user manually performing actions such as starting the mobile application to become aware of the state of remote computers and terminals is referred to as pull because a user action triggers or "pulls" the information for display to the phone.

Multimedia audio and video presentation applications, Voice over IP (VoIP) communications, multimedia interaction applications, games including games which involve other player and automated server actions such as game events and challenges from other mobile terminals, mobile business process applications, real time back office connectivity applications and corporate mes-

saging programs are examples of areas where mobile terminal applications benefit from the ability of server placed arbitrarily on the public Internet having the ability to initiate the display of or remotely configure the view presented by an already running program on a mobile terminal at any time. Due to technical limitations of the terminal and user preferences, it is generally not possible for a mobile terminal to support multiple such large or resource-intensive applications running continuously. Therefore there is a need for a more general solution to automatically install, update, provide data to, launch and configure these applications from the background on mobile terminals on any mobile network.

Commanding an application on the mobile terminal, launching an application with parameters specified in the launch message so as to view specific information after the program starts, changing the current view of an application which is already running, pushing or pulling new information into an application so as to change what is presented to the user are all referred to herein as changing the state of the application. This application state change process generally requires personal initiative and several manual and cumbersome steps and decisions on the part of the user: opening the application or changing the view of the application, selecting and then examining the content to see if any of the changes are of interest. Because of the limited size, network bandwidth and user interface of mobile terminals, performing these steps is significantly slower on a mobile terminal than performing the same actions on a larger computer. The process of checking if an application should be launched now because new and interesting Internet information might be available is therefore less interesting to mobile terminal users than on a larger terminal because of the limited capabilities of the mobile terminal to rapidly display many alternative content formats. This frustrating or slow user interface with for example small buttons, touch screen or relatively slow interface response on the mobile terminal is one of the reasons there is commercial need for eliminating the user steps and push commanding the mobile application remotely from a server only when new and interesting information is available.

Given the shortcomings in the prior art, there is a need for a method whereby a computer on the Internet can rapidly and at reasonable cost be permitted to at any time initiate control of one or more applications on an individual's mobile terminal to deliver through that mobile application real time in-

formation, interactivity and rich media content, regardless of which mobile operator is being used and where the mobile user happens to be at that moment.

Brief description of the invention

An object of the present invention is a new technique for providing a push-type command of applications on a mobile terminal by a remote server computer. The object is achieved by the invention is characterized by what is stated in the attached independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

In a preferred embodiment of the present invention is a system and method for a server placed freely on a connected network outside the wireless network firewall or other corresponding wireless network security entity, to push messages to a mobile terminal located in the wireless network and thereby cause programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message thereby presenting a new application view to the user of the mobile terminal. The mobile terminal is provided with means, such as software, which initiates and maintains contact with the server using Internet technologies, thereby avoiding cost, latency, contractual and firewall penetration issues of the server contacting the mobile terminals by telecommunications messaging or Internet technologies. This mobile-initiated permanent IP connection allows the server to pass or push messages from outside the operator's firewall to the mobile terminal at any time. If the server would attempt to use IP to contact the mobile device directly, the attempt would fail due to the firewall(s).

In an embodiment of the invention, the mobile terminal maintains contact with the server by periodically testing the connection with a suitable keepalive message, a "ping", which resets timers in intervening operator stateful firewalls and/or NAT (network address translation) firewalls. The mobile terminal may also automatically re-establish the connection when the connection gets broken and adjust its connection settings based on past experience with failure to connect and such broken connections in a given mobile network.

In an embodiment of the invention, the push messages may include, for example, a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface feature of the terminal such as an application which is part of the basic terminal software or and an additional installed application beyond the base software supplied with the mobile termi-

nal. In response to receiving such a message, a mobile terminal may spontaneously open the application, dynamically loaded module or user interface feature of the terminal thereof to a designed application view or location, present new information of the availability of new information, a new feature or operating state. If such application, module or user interface features is already operating in the mobile terminal, the action of such a message would instead stimulate the application or user interface feature to present itself to the foreground of the user interface and change state as specified in the application-specific message received from the server. In further embodiments of the invention, push messages may include, for example, messages triggering the mobile terminal to play a sound notifying the recipient of the application command or state change, or display notification providing event information from which the user may select or decline to display the application.

Note that in some cases the packaging of mobile applications involves combining multiple applications delivered in a single bundle or application suite preinstalled or later installed to the mobile terminal. Commanding the display of an additional, more resource-intensive user interface feature such a rich media, or highly interactivity modes within the same bundle of applications or application features as for example by explicitly or implicitly loading or calling an additional library such as a user-interface related code or other embodiment of an application on a mobile terminal within the same application based on push event messages recently received from an IP connection is simply an alternative packaging of this same invention. For brevity herein, this type of commanding of a new user interface modes or view to appear within the same application suite is considered and discussed as the commanding of a new application since the packaging of rich user interface features and program modules within a bundle or separately is a relatively minor detail in the embodiment of the invention.

The cost for a user's mobile terminal to maintain a connection to the push server and receive such messages over mobile Internet connections is minimal, thereby solving the problem of some mobile information services not being economic to offer. The advantages are: all the convenience of standard push services such as SMS-based application launch and command together with the mobile network-independent and economic benefits of placing the server outside of any single operator's network and of the service provider not having to pay an operator or operator middleman per command event.

IP push messages utilizing the principles of the invention are delivered rapidly, bypassing the public and often crowded SMS, MMS, WAP Push and email store-and-forward mechanism within an operator and between operators. This guarantee of very rapid event push provides usability benefits to users which may be then designed into the mobile applications. For example the ability to expect prompt delivery allows modification to interactive mobile application system design. The mobile process surrounding the application can be changed such that a user on one mobile terminal may take actions which result in the initiation of a push event to a user on a second terminal and then wait for a short time for the second user to respond after the launching or commanding to return to be the focus of user interface attention their copy of the same, similar or complimentary mobile application function involving Internet communication directly or mediated by a server between the two mobile applications.

The advantages of performing push service application command in accordance with the present invention include the ability to run such a service from outside the mobile operator's firewall and gateway devices, skip the overhead charges like per-message SMS fees normally associated with "mobile push", and make it easy to create mobile applications as web pages, therefore usually without programming. Thus, push application command services according to the invention can be modified from existing or newly designed mobile applications, modules and application features simply by creating an application command, module or feature entry point compatible with the embodiment of the push client. This embodiment can be, but is not limited to, a separate application, operating system background process or application module bundled in a suite with the mobile application and kept running such that it may receive IP push events and command applications, modules or significant application features.

These messages may be routed automatically to a nearby computing device with faster or less expensive network connectivity such as a broadband access point, server or workstation in the proximity of the mobile terminal. Both mobile terminal and access point must be equipped with a wireless communication network such as RFID, Bluetooth, ultrawideband, Zigbee, Wi-Fi, Wi-Max or other personal area, local area, metropolitan area or large area network. This ability embodied in the invention alleviates speed and economic problems that affects the present-day mobile messaging solutions which are either limited in bandwidth or cost based on volume of use. When in proximity to a more

capable network, if a connection can be established to this alternative broadband network access point, it is used preferentially and intelligence normally located in this broadband access point would route messages received on behalf of the wireless terminal to and from the server. Further, the availability of a broadband access point would be notified to mobile terminal application software and server alike allowing either to initiate bandwidth intensive operations such as application update and application data update.

IP push command messages may be triggered either by events which the server is aware of, or events which a similar mobile application on another mobile terminal is aware of and which that push client makes the server aware of, the server in turn initiating a push command event. Such client-side events of which the server is informed for the possibility of delivering new web services include the making, receiving, and termination of telephone calls, the transition from presence-to-absence or absence-to-presence of other devices in a geographical area, metropolitan area, local area or personal area wireless communications network, mobile terminal creation of photographs video audio or other media, mobile terminal presence of files matching a given filtering criteria, changes in internal state of electronic equipment, taking of measurements, processing of such measurements to see if they match certain criteria, video game actions or events, application calculation events and messaging actions. In some cases a separate server such as a telecommunication service server, gaming environment server, and original equipment manufacturer device or business information system may notify the server directly of events or messages to be sent using an external application programming interface (API). Such a device connected by external API may also receive information including the results and responses of messages which the user has replied to by terminal software or web page interaction.

The invention provides content and application producers with a cost effective, network-independent and device-independent service for the rapid creation and distribution of interactive information alerts and Internet launch-at-will and present-when-needed features for their users.

The invention provides techniques for launching and changing the operating state such as information currently presented to the user of applications on a mobile terminal at will by a server computer and without the need for any additional action by the recipient, and more specifically to a system, method and program for sending, receiving and acting upon messages sent to a mo-

mobile client device over a packet switched data network for the purpose of initiating application launch, application command, module or feature display and user direct or indirect user interface state change based on server-side events and mobile terminal events including user interface events, phone calls and network proximity events, and local resource changes.

Brief description of the drawings

In the following description, reference is made to the accompanying drawings which form a part hereof, and which illustrate several embodiments of the present invention. In the drawings:

Figure 1 shows an implementation known in the art for pushing information including commands to an application through existing telecommunications SMS infrastructure to a mobile terminal and if necessary launching the application;

Figure 2 shows an implementation known in the art for pushing information including commands from inside the mobile network firewall to an application to a mobile terminal and if necessary launching the application;

Figure 3 shows an implementation known in the art for pushing information including commands from outside the mobile network firewall through a firewall hole opened by the mobile network operator to an application to a mobile terminal and if necessary launching the application;

Figure 4 is a block diagram illustrating an exemplary implementation of the system for pushing mobile application launch commands to a mobile terminal based on server side events in accordance with one embodiment of the present invention;

Figure 5 is a block diagram illustrating an exemplary implementation of the system for a wire terminal with an alternative broadband connection to use the alternative broadband access point for receiving push messages including launch events, application updates and data updates;

Figure 6 is a flow chart illustrating an exemplary process by which the mobile terminal maintains an open path for network communication with the server (6A), keeps the connection to the server open and tests the integrity of the connection while automatically reestablishing the connection as necessary (6B), responds to messages from the server (6C), and notifies the server of locally monitored events on the mobile terminal (6D) in accordance with one embodiment of the present invention;

Figure 7 illustrates an example of a "COMMAND PUSH" procedure;

Figure 8 illustrates an example of a "COMMAND PUSH WITH BIDIRECTIONAL DATA" procedure;

Figure 9 illustrates an example of a "BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA" procedure;

Figures 10A, 10B and 10C are flow diagrams showing examples of processes by which the server maintains a connection with the client and communicates commands and data to it.

Detailed Description of the Invention

In the above description, the invention is described using various embodiments of the present invention as examples but the invention is not intended to be restricted to these embodiments. It is understood that other embodiments may be utilized and structural and operational changes may be made without departing from the scope of the present invention.

Figure 4 illustrates an exemplary implementation of the system for pushing application commands to a mobile terminal based on server side and client side events in accordance with one embodiment of the present invention. More specifically, Figure 4 illustrates a Push Client basic functionality 405 implemented in a mobile terminal 404 as part of a message passing system in cooperation with a Push Server 401. The push client 405 is preferably implemented in the form of a software run in a processor of the mobile terminal 404. The mobile terminal 404 is preferably a commercially available mobile terminal, such as a portable phone or appliance capable of running software or personal digital assistant, which provides a platform for downloading application software over air or from a personal computer, installing the software in the terminal, and running the software in the terminal. For example, the Symbian operating system is an open operating system, application framework, and application suite optimised for the needs of wireless information devices such as intelligent phones, smartphones and communicators, and open operating system and drives standards for the interoperation of data-enabled mobile phones with mobile networks, content applications, and services. The Symbian operating system also includes connectivity software for synchronisation with data on personal computers and servers. The application may be in an appropriate programming language, such as C++ or Java, which is an object-oriented pro-

gramming language and virtual machine platform developed by Sun Microsystems.

The push client software 405 preferably launches automatically when the mobile terminal 404 is turned on. The push client software 405 runs in the background and attempts to log into the push server 401 over a data network 403, normally a wireless network capable of transmitting Internet Protocol (IP) packets. The arrow A in Figure 4 illustrates an optional attempt by the push client 405 to communicate with the wireless network firewall 402 or other similar security or gateway device in order to open a connection for the push server 401 to directly contact the push client 401 as in FIG 3. If successful, operations can continue as described in FIG 3 or as below. Arrow B illustrates a login attempt.

The wireless network 403 may be protected by means of a firewall or other appropriate security entity 402, which connects the wireless network to the public networks and filters and selectively discards the data packets entering and exiting the wireless network according to predefined rules. Thus, a firewall is a gateway device which operates at the same time as a connector and a separator between networks in a sense that it keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Additionally, IP connection techniques, such as Internet Protocol 4 (IP4) network address translation and Internet Protocol 6 (IP6) security, encryption and/or authentication, may hide the actual address of the mobile terminal or make it otherwise difficult for a server to connect to directly to the mobile terminal. The public telecommunications operator, company, organization, or private individual setting up this mobile Internet space with one or more users having greater ability to contact one another and included servers does this to protect the mobile terminals from hostile or unwanted contact common on the public Internet. They may also do so to reduce background traffic, protect their control over this space and limit outside or undesired service providers through technical connection policies set in the firewall, gateway or other security device. Physically a firewall may be a machine with appropriate software to do the task assigned to it. 402 can be a firewall, router, a personal computer, a gateway server or whatever similar computing device, infrastructure or secure protocol such as IP6 can be used for such purposes.

Consequently to the existence and configuration of 402, if a fixed or mobile computing device from outside the controlled mobile network tries to contact a mobile terminal 404 inside the controlled mobile network, the incoming connection is not generally permitted unless the organization or individual controlling the firewall, gateway server or security device 24 makes an adjustment to their security policy and explicitly allows the connection.

From point of view of the wireless packet data network 23, the login attempt B and associated connection establishment C is one or more normal IP connections established at the request of the mobile terminal. If optional attempt A to open a path for the push server 401 to initiate the IP connection now or in the future, use from that point forward may proceed as in FIG 3. However this firewall and/or security device or protocol opening A is unsuccessful, the login attempt B is in either case normally allowed to pass the firewall or security infrastructure 402 since the connection is from the inside the firewall to outside.

After attempting login, if the login is not successful the client 405 may automatically or under supervision of the user of the mobile terminal 404 try several different techniques for contacting the server 401. Since there are numerous variations between mobile terminals and in network connectivity, more than one connection attempt may be needed to contact the push server 401. Differences in wireless network terminal characteristics, individual push server availability and accessibility, firewall and gateway permissions, connection timeouts, connection level stateful (such as TCP) and stateless (such as UDP) transport protocol availability (such as IP4, IP6, SSL, HTTP, HTTPS) and alternate mobile terminal network settings mean that a sequence of connection establishment attempts and connection maintaining steps may required to be made using variations in relevant network parameters.

A second reason for automatically adjusting the network parameters is not simply establishing the connection but establishing the connection in the most cost effective or highest performance configuration available for the individual mobile terminal user account service level. Connection types differ in speed, customer expensive, server resource usage and hence scalability, security and ability to penetrate gateway security devices. Some customers may be offered more secure or higher performance service while others receive the least cost connectivity from either the mobile terminal's or the push server's standpoint.

As an example, such network parameters may include but are not limited to one or more of the following:

- Use of a connection-oriented protocol suitable to the wireless network such as TCP/IP protocol, which is generally preferred in the common situation where an intermediate firewall, Network Address Translation (NAT) or gateway device 402.

- Use of a connectionless protocol suitable to the wireless network 403, such as UDP/IP, which is generally preferred when no network device restricting terminal contact 402 is present as this reduces resource usage on the server when large number of mobile terminals is served.

- Use of an alternate connection-oriented protocol such as HTTP suitable for mobile push operation through more strict firewalls and proxy Internet connections.

- Use of a secure protocol such as HTTPS, IP-Sec, secure IP6 or a proprietary security protocol to identify the communicating parties, prevent message interception by 3rd parties, and prevent message modification by 3rd parties.

- Use of a periodic message from the client to the server or server to the client to the effect that client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices do not time expire the connection.

- Use of configuration messages to the firewall (FIG 4, A) using a firewall or other security configuration protocol, such as Universal Plug and Play, to open a path for server-initiated connection-oriented or connectionless messaging to the client.

- Use of periodic messages initiated by the client 405 or by the server 401 to the effect that the receiving application is informed that their messages are continuing to be received, as indicated by response data from the receiving party to the sending party.

- Use of longer or shorter timing between such periodic messages to match the combined needs of all such network devices and protocols involved in transmitting communication, as adjusted based on the success or failure of earlier messages to successfully traverse the open network connection.

- Use of an alternate push server network address such as an address accessible with fewer security and performance restrictions which may be more available, more accessible, lower cost, lower latency, less busy, higher

bandwidth or otherwise preferred at the present time and from the present network location of mobile terminal 404.

- Use of one or more alternative mobile terminal network connection settings, or variation of the parameters within the settings.

- Use of an alternate connection route through a second mobile or fixed terminal accessible to the mobile terminal over an alternate wireless network or network connection and capable of communication with a push server.

In an embodiment of the invention, the mobile terminal 404 keeps a prioritized data structure listing the preferred communication protocols, server addresses, periodic message timings, network access settings, and alternate communication routes which it should use. Automated and manually assisted use of this structure should then result in a connection to one or more push servers, however if one of these connections which the mobile terminal is programmed to expect is not available, the mobile terminal can choose the sleep that function of the client software and attempt re-connection at a later time, repeating in like fashion with the same or different network connection parameters as described above until a connection is established or other user intervention.

At any time after a connection is established between the client 405 and the server 401, the client may push a message to the server or the server may send a push message to the client. This is illustrated by means of the arrow C in Figure 4. These messages through a previously established, connection-oriented protocol such as TCP/IP, SSL, HTTP or HTTPS arrive quite rapidly, more rapidly than if the connection were established only when needed. The associated protocol overhead such as 3-way handshake during connection establishment thus occurs before the actual need for message transmission rather than needing to occur at time of transmission and thus delaying the transmission.

A connectionless protocol, such as UDP/IP, may also be used in cases where the connection-oriented protocol is not possible or not desirable because of the push server resources used by every static instance of a connection-oriented protocol. Connectionless communication is also used when a message needs to get through to the server 401 quickly, such as when occurs when the client 405 notifies the server 401 of a terminal event, user interface event or application event but the connection-oriented protocol connection is not connected or is already busy transferring information. Such a selective use

of this high priority, low latency communication channel from terminal 404 to server 401 gives the server the opportunity to in return push to the client 405 a service triggered by the event begin communicated by the client 405 as will be described in more detail below. The sending of such a return message is frequently time critical and the fastest available combination of techniques will be used.

In the preferred embodiment of the invention, the most basic message pushed from the server 401 to the client 405 is a data packet containing no information. Additional binary or text information specifying which mobile application 406 from a plurality of such applications may optionally be included. Additional binary or text information to be passed to the default or specified mobile application may optionally be included. Additional binary or text information specifying how upon receiving such a message the client 405 will notify and optionally ask the user if the action should be performed may optionally be included. Upon receiving such a message, appropriate automated actions and user interface media capabilities of the mobile terminal as specified in the command C from the server 401 are executed by the push client 405. The most common case is playing a sound, asking the user if the mobile application should be launched, and if affirmative passing the command details (arrow D) to the specified mobile application, module or additional feature within the same application suite, launching the application, module or feature if needed. Such action may include optionally proceed without audio, with network downloaded audio, or without first requesting confirmation from the user as specified by user preferences and command details.

The push message from the push server 401 may be triggered by any trigger event, local or remote, defined at the server. The trigger may, among others, include an alarm, notification, or measurement result received to the push server 401 from another device or system. With a push message, the server 401 may direct the mobile application 406 to make use of additional network resources either on the push server or other server. The push client 405 may in turn at any time accept data D from each of a plurality of mobile applications 406 and direct such to the push server 401, possibly for redirection through push server API to other servers, mobile terminals, push clients and computing devices.

Figure 7 illustrates an example of an "COMMAND PUSH" procedure wherein the push server 701 is triggered by a trigger event as for example from

an application server 702 to push an application command message to the push client 704 and thereby initiate a mobile terminal client trigger event in a mobile application 705 from a plurality of such applications, program modules and user interface features on the terminal 705. The trigger event from push client 704 to mobile application 705 may optionally include commands or data affecting the aspect of visual presentation of mobile application 705. The even trigger mechanism may be any electronic process mechanism as for example computer software calls to load or configure a class, library, dynamic link library, MIDlet, Symbian application, Linux daemon or other executable object. The trigger mechanism may be between separate parts of a larger application or application suite, or may be an IP-triggered application launch and data transfer as in the case of mobile application launched by contact to a specified IP port. The potential applications of the COMMAND PUSH include but are not limited to mobile applications for enterprise connectivity, back office integration, database access, scientific and industrial process and equipment monitoring and control, pictures transfer, mobile gaming, application data transfer, mobile electronic commerce, application alarms, reminders, multimedia interactivity, corporate calendaring, personal messaging and group messaging, etc.

The push server 701 may in combination with user preferences stored in either the push server 701 or push client 704, optionally request the push client 704 to display or otherwise as appropriate for the mobile terminal or appliance notify the user asking permission for launching mobile application 705 prior to application launch. The preferred embodiment is for the behavior, language and content of this information to be configured on the server 701 based on the service and preferences of the individual receiving the message. In such cases an optional informational message will be presented to the user and such information messages are associated for instance with the menu option transmitted to the client 704 by the server 701.

In an embodiment of the invention, the client 704 is also capable of receiving and storing variables which configure behavior of the client 704. The server 701 may thus specify the network connection preferences, notification sounds, and other behavior of the client 704. These changes facilitate the efficient and manageable operation of the entire system and can be used for automated remote maintenance of push client 704, mobile applications as 705, and configurable aspects of underlying mobile terminal 703, for example

changing the username, password, and security certificates stored in the mobile terminal.

Figure 8 illustrates an extension of the procedure in Figure 7, one known as "COMMAND PUSH WITH BIDIRECTIONAL DATA". This embodiment of the invention includes all aspects of "COMMAND PUSH" with the additional step that a data connection between application server 802 and mobile application 805 is established with the aid of the persistent managed, tested and configured data connection in Figure 4, arrow C between push server 401/801 and push client 405/804. An IP or other API (application programming interface) connection between application server 802 and push server 801 simplifies the work and cost of creating application server 802 by taking care of network details already established for the COMMAND PUSH procedure. Similarly, an IP or API connection between push client 804 and mobile application 805 completes the connection and reduces the number, cost and resource usage of a possible plurality of such connections for a corresponding plurality of mobile applications. Further, each mobile application 805 is now free to sleep, exit or otherwise release the limited resources of the mobile terminal 803 with the assurance it may be remotely commanded back into action provided at least one push client 804 from a possible plurality of such push clients remains active, connected to the push server 801 and configured to launch the mobile applications 805.

Referring now to Figure 5, users of mobile terminals 507 are frequently but not continuously in range of alternative and more desirable wireless network access (Figure 5, arrow A). Such access is shown in the exemplary embodiment as broadband access point 509 within alternate and more desirable for reasons such as speed, cost and security broadband wireless network 507. Such an access point 509, which may also be mobile, is referred to herein as a broadband access terminal. The push client network connection functionality according to the invention may also be installed on such a broadband access point to facilitate routing and connection over alternative wireless network 507 such as a bluetooth, Wi-Fi, Wi-Max, Zigbee, radio frequency, infrared, ultrawideband, grid network or similar opportunistic or ad-hoc wireless network. Thus, both devices 508 and 509 have the minimal capabilities of client software 405 necessary for establishing and maintaining the already established contact with push server 501. Further, the two devices detect one another and so noting inform the server 501 through connections B or C and are thereafter

temporarily associated with one another in the server for routing and mobile application launch and data transfer purposes. Further, the push server 501 on becoming aware of such a situation may inform (arrow D) the application server 502 of the availability of a more desirable network connection (C plus A) to the client and on behalf of the application server 502 or independently decide to push additional commands and data to the wireless terminal using this connection. Further, the push client in the broadband access point has the additional capability to route such information to the wireless terminal. The result benefits customers using the wireless terminal in that data is managed and updated automatically for their mobile applications in the most cost efficient manner for non-time-critical capabilities such as lazy application code update and lazy application data update. While such alternative routing may also be achieved through normal IP routing and path cost without the presence in the broadband access point 509 of push-aware client software, the push server 501 and application server 502 would in this known-in-the-art implementation not be aware of when the low cost alternative route was available and thus able to at such time trigger the push of lazy application code and data installation and updates.

Figure 9 illustrates an example of a "BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA" extending the earlier discussed "COMMAND PUSH WITH BIDIRECTIONAL DATA" disclosed in Figure 8. This procedure wherein the push server 901 has been earlier informed by either the mobile terminal push client 906 or broadband access point 904 of the available alternative broadband network 507 and associated route (Figure 5 D, C and A, corresponding to Figure 9 A, B and C). Based on this notification and user preferences the push server 901 may choose to route future messages to either device, however the preferred remote application command push and data route is indicated by arrows B and C. Then at some later time the push server 901 is triggered by a trigger event of which the application server 902 is aware to send push message to the mobile terminal 905, and procedure steps A, B, C are traversed thereby pushing application launch commands, lazy application updates, and lazy application data updates through push clients 904 and 905 to mobile application 907 through local command and data path D (also Figure 5, arrow A).

Figures 6A, 6B, 6C and 6D are flow diagrams showing examples of processes of the preferred embodiment by which the client 405 maintains a connection with the server 401 and communicates messages to it.

Firstly, in step 602 the push client 405 initiates an attempts to log into the push server 401 over data network 403, as indicated by the arrow B in Figure 4. Success of the connection attempt is monitored in step 603, and if the network connection shows an error or does not get a response from the server in a reasonably short time the network settings are adjusted in 604 (for example in the manner describe above if the network connection fails). If the server does connect but login fails at 605, the push client may change the login settings in step 606 (for example in the manner described above if the login is rejected) and retry the login. If the login to the push server 401 is successful, a connection is already opened to the client 405 and the application server 405 changes state informing applications server 502 from a plurality of such server of the availability of the client 401 and relevant details. Thereafter the mobile applications 406 of a plurality of such applications can be contacted until the server 401 is otherwise notified or decides based on exceptions in network communications that the terminal 404 has disconnected.

In association with the login procedure the client 405 may attempt to communicate with the mobile network firewall, gateway or security device 402 it is behind using a firewall configuration interface, such as the Universal Plug and Play (UPnP) Internet gateway configuration protocol (the arrow A in Figure 4). In an alternative embodiment t may do so either before step 601. In either case the client 405 requests the firewall 402 to open an IP hole allowing the server 401 to initiate contact with the client 405 whenever there is need a need thereafter allowing classic prior art mobile application launch as illustrated and described in Figure 3. In the preferred embodiment, the configuration of the firewall 401 to allow incoming messages in this manner is attempted in step 607 immediately after login, and if the security opening operation appears successful (step 608) the server 401 is notified by the client 405. The server 401 then attempts this type of direct IP connection to the client 405 or mobile application 406 (step 609), and if that too is successful (step 610), then one of these test connections is closed and both server 401 and the client 405 mark the second connection as closable (step 611) since they now know that they may save bandwidth charges and resources by closing the connection knowing that server 401 has now gained the ability reopen the connection when

needed for a classic command push procedure (Figure 3, arrow A) or other data communication use. At any time after this point the server 401 or the client 405 may choose to close the remaining network-level connection (usually a TCP or SSL connection) while keeping the application-level "connection" in the form of knowledge of how the server 401 can contact the client 210. The advantage of such an application-level connection without the network-level connection is lower use of network resources particularly on the server side thus significantly increasing server scalability for infrequent command and data push applications by decreasing overhead cost per active user.

Referring to steps 620 and 621 in Figure 6B, after the login and connection setup in Figure 6A, the push client 405 may send a periodic message (the arrow C in Figure 4) from the client 405 to the server 401 to the effect that client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices do not time expire the connection. The period of time (measured in seconds, minutes or hours and varying from mobile network to mobile network) between such periodic messages is set to match the combined needs of all such network devices and network protocols involved in transmitting communication (step 604). The client 405 may then wait for a reply or acknowledgement from the server 401, and if the acknowledgement is received (step 622), the client 405 returns to step 620 to await the next combined connection refresh and test. If the no acknowledgement is received, the client 405 may return to step 604 in Figure 6A to possibly automatically adjust network settings or, if it deems the settings correct but the network not available, simply re-attempt login to the server 401.

Referring to Figure 6C, after the login and connection setup, the push client 405 is ready to receive the push messages over the connection from the server outside the operator's firewall (step 631). If a push message is received, the client 405 executes the corresponding function, such as launch or pass commands and data a mobile application (step 632). If required, the client 405 may also send a message to the server 401 (step 633), such as a command execution acknowledgement or result.

Referring to Figure 6D, after the login and connection setup, the push client 405 may monitor the local resources for a state change (a trigger event) in step 641. If a state change of other event is detected in step 642, the push client 405 may send a message to the server 401 (step 643).

The push server 401 can be server software run on any appropriate computing device. Figures 10A, 10B and 10C are flow diagrams showing examples of processes by which the server 401 maintains a connection with the client 405 and communicates push commands and other data to it.

In step 1001 of Figure 10A, the push server 401 receives a login from the client 405 initiates an attempt to log into the push server 401 over a packet switched network 403, as indicated by the arrow B in Figure 4. In step 1002, a connection is opened to the server 401 and the server 401 is informed of the client's its availability and the details by which the client 405 can be contacted until the server 401 is otherwise notified or detects a network fault or shut-down. In step 1003, the server 401 attempts this type of classic IP push connection to the client 405, and if that is successful (step 1004), then one of these connections is closed and both the server 401 and the client 405 mark the second connection as closable (step 1005).

Referring to steps 1010 and 1011 in Figure 10B, after the login and connection setup, the push server 401 may receive a periodic message (the arrow C in Figure 4) from the client 405 to the effect that the server updates the respective server object associated with a given client so that the connection, server socket or client socket is not time expired as being stale. The server 401 may send a reply or acknowledgement in step 1012 to notify client 405 of successful network, firewall and security traversal.

Referring to step 1021 Figure 10C, after the login and connection setup, the push server 401 monitors for trigger events and event messages. If the server 401 is triggered by a trigger event (the result "yes" in step 1023), it decides based on application-specific logic and/or user preferences whether the resulting push procedure is a BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA procedure in step 1024. In case of BROADBAND COMMAND PUSH WITH BIDIRECTIONAL DATA, the server 401 sends the command or data push message to the push client 508 through the push client 509 (step 1025). If not using this alternative network connection selected in step 1024, the push server 401 proceeds to step 1026 to perform a more classic COMMAND PUSH or COMMAND PUSH WITH BIDIRECTIONAL DATA. In case of COMMMAND PUSH, the server 401 sends an command push message to the push client 405 and thereby forces a mobile application 406 from a plurality of such push-aware mobile applications in the mobile terminal as specified in the command (step 1026). In the case of COMMAND PUSH WITH

BIDIRECTIONAL DATA, the push server 401 sends the client 405 push commands or data and may return response through the same IP connection (step 1026).

If the server 401 is not triggered by a trigger event (the result "no" in step 1022), it checks whether an event message has been received from the client 405 (step 1023). If not, the process returns to step 1021. If an event message has been received from the client 405, the server checks whether a proximity detection is involved indicating that the mobile terminal 508 can connect to a broadband access point 509 (step 1024). If the broadband access point 509 is connectable, the server 501 performs accordingly, typically by sending an command or data push directly through the broadband access point in a manner described with reference to Figures 5 and 10C (step 1025). If the alternate broadband connection is not available or not preferred in preferences, the server delivers the message directly as above (step 1026).

The above specification, examples and data provide a complete description of the manufacture and use of the system, method, and article of manufacture, i.e., computer program product, of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

Claims

1. A method of pushing commands and data to a wireless terminal from a push server located outside a wireless system serving the wireless terminal, comprising

the push client initiates and maintains over an extended period of time a packet-based data connection through at least one communication security or inter-network connection device of the serving wireless system to the push server using Internet technologies;

the push server sends, in response to predetermined trigger events, at any time push application installation, updates, commands or data messages to be directed to a push application or dynamically loaded module or user interface feature from among a plurality of such applications, modules and features by means of said client-initiated or client-opened and client-maintained permanent connection, whereby avoiding blocking of said server-originated push messages by the security device, and launching said application, application module or dynamically loaded module or user interface feature as needed,

the push client, in response to receiving a push message containing application installation, updates, application commands or data from the push server, forwards such application commands or data or stores such application installation or updates within the mobile terminal to a mobile application from among a plurality of such applications so as to initiate launch optionally to a specified state or if already running initiate or change presentation to the user according to the push message.

2. A method as claimed in claim 1, comprising

the push client sends configuration messages of a security device configuration protocol to the security device to open a path for later server-initiated connection-oriented or connectionless messaging to the push client.

3. A method as claimed in claim 1 or 2, comprising

the security device is a security protocol such as IP6 whereby the client may open the possibility for the server to contact it by exchanging security keys or otherwise enabling subsequent server-initiated contact.

4. A method as claimed in claim 1, 2 or 3, comprising

the push server attempts server-initiated messaging through the security device to the push client after having being informed of the client-initiated connection.

5. A method as claimed in claim 1, 2, 3 or 4, comprising

the push server and the push client after testing the ability of the server to open a connection to the client mark the maintained network-level connection closeable,

the push server and the push client can close said network-level connection while keeping an application level connection information indicating future possibility for the push sever to reopen said network-level connection when needed.

6. A method as claimed in any one of claims 1-5, wherein the step of maintaining further comprises that the push client maintains the permanent connection through the security device by sending periodic keep-alive messages.

7. A method as claimed in any one of claims 1-6, comprising
the push client or the push server sends a periodic reply to messages initiated by the push server or by the push client, respectively, to the effect that the receiving end is informed that the messages are continuing to be received.

the push client or the push server upon failure to receive acknowledgement of said periodic reply may choose to open a new connection.

8. A method as claimed in claim 6 or 7, comprising
use of varying timing between the periodic keep-alive or reply messages to match the combined needs of various network devices involved in transmitting and maintaining communication.

9. A method as claimed in any one of claims 1-8, comprising
if an attempt to contact the push server during initiation of the permanent connection and login is not successful, the push client automatically or under supervision of the user of the wireless terminal tries one or more other techniques, protocols and/or network parameters for contacting the push server.

10. A method as claimed in claim 9, wherein said trying of one or more other techniques and/network parameters include one or more of

using an alternate push server network address which may be more available or more accessible at the present time and from the present location,

using one or more alternative mobile terminal network connection settings, or variation of the parameters within the settings,

using an alternate connection route through a second wireless or fixed terminal accessible to the wireless terminal over a wireless network and capable of communication with the push server,

using a TCP connection,
using a UDP connection,
using an SSL connection,
using an HTTP or tunneling HTTP connection,
using an SHTTP or tunneling HTTPS connection,
using an XML-based connection over other transport protocol.

11. A method as claimed in any one of claims 1-10, comprising the push client stores in the wireless terminal a prioritized data structure listing preferred communication protocols, server addresses, periodic message timings, network access settings, and/or alternate servers and communication routes and uses this data structure to attempt reconnection to the push server if the connection to the server fails.

12. A method as claimed in any one of claims 1-11, wherein the connected networks on which the push server and mobile terminal are located are private networks which allow greater interconnectivity than they both offer to the public Internet.

13. A method as claimed in any one of claims 1-12, wherein the message the push server sends to the push client includes an application launch or reconfiguration push message directing the immediate or subsequent actions and data of the application.

14. A method as claimed in any one of claims 1-13, wherein the push server sends to the push client include an application command or data or reconfiguration message redelivered by the push client as an API call or IP connection between processes running on the same mobile terminal.

15. A method as claimed in any one of claims 1-13, wherein the push server sends to the push client is new application code, application code updates or application data updates.

16. A method as claimed in claim 13-15, wherein the push client is a library or process installed independently or together with but containing or enabling the functionality to supply push messages to one or more of a plurality of applications, modules or dynamically loaded module or user interface features on the mobile terminal.

17. A method as claimed in claim 16 wherein only one of the possible plurality of push clients need operate at a given time, providing push services for a plurality of push-aware applications on the mobile terminal.

18. A method as claimed in any one of claims 1-17, wherein the message the push server sends to the push client includes an optional application launch or event push message triggering the wireless terminal to play a sound notifying the recipient of the message and/or to display notification information such as text, rich text, graphics and rich media from which the user may select or decline to launch the application, dynamically loaded program module or user interface feature based on push message or messages recently received.

19. A method as claimed in 18, wherein the notification sound, text, rich text, graphics and rich media presented by the terminal is selected by and deliverable from the server and may be retrieved from the server by the terminal, thereby allowing the push server to indicate through audio and media signals including note sequences, audio samples sound modification applied to note sequences and audio samples, spoken speech, color, motion, shape and design the message sender, nature, priority, content and other attributes of the received message, message sender and/or message sender current state.

20. A method as claimed in 19, wherein the specified notification information and media is played from a cache in the terminal and the cache is automatically updated over the air as needed with new notification information and media.

21. A method as claimed in any one of claims 1-20, wherein said trigger events include events which the push server is aware of and/or events which the push client is aware of and which a push client from among a plurality of such push clients makes the push server aware of.

22. A method as claimed in any one of claims 1-21, wherein said trigger events include one or more of: the making, receiving, and termination of telephone calls, the transition from presence-to-absence or absence-to-presence of other devices in a physical contact, RF, near field, infrared, personal area, local area, metropolitan area or geographical area wireless communications network, an alarm, notification, videogame action or event, remote application user or application server event, remote user action or inaction, electronic or computing equipment change of state or measurement result.

23. A method as claimed in any one of claims 1-22, comprising the push client in the wireless terminal detects availability of an alternate wireless network connection to a broadband access terminal, or the broadband access terminal detects ability to initiate contact to the wireless terminal,

the push client is responsive to receipt of command and data, application installation and update push messages through said broadband access terminal.

24. A method as claimed in any one of claims 1-23, comprising

the push client in the wireless terminal detects network connection availability of a terminal device with a higher bandwidth capacity or otherwise specified as preferred, or the device with a higher bandwidth capacity detects such ability to connect to the wireless terminal

the push client transmits connection availability information of the higher bandwidth device to the push server, or the large bandwidth terminal transmits connection availability information of the mobile terminal to the push server,

the push server uses the connection availability information as a trigger event for sending lazy or low priority messages including application updates and application data updates routed through the higher bandwidth capacity device to the wireless terminal.

25. A method as claimed in any one of claims 1-24, comprising

the push client in the wireless terminal detects connection availability of a higher bandwidth or more desirable alternate network connection device,

the push client transmits connection availability information of the higher bandwidth device to the push server,

the push server uses the connection availability information as a trigger event for routing messages directed to the user of the wireless terminal through the higher capacity device.

26. A method as claimed in claim 25, comprising

the push server stops directing messages to the higher capacity device when the wireless terminal is no longer connectable to the higher capacity or more desirable alternate wireless network connection device.

27. A method as claimed in any one of claims 24-26, comprising

providing the higher network connectivity device with a push client with server connectivity similar to that in the wireless terminal.

28. A method as claimed in any one of claims 1-27, comprising

the push client in the wireless terminal detects connection availability of a device with a better alternative network connection, or a push client in the device with a better alternative network connection detects connection availability of the wireless terminal,

establishing a data-transfer capability between the push clients,
routing communication to and from the push client in the wireless terminal through the push client and the network connection of the better alternative network connection device.

29. method as claimed in any one of claims 1-28, comprising
customizing the appearance, notification sound or look and feel of the messages received to based on message source, message source state, message parameters or message recipient preferences.

30. A method of pushing messages to a wireless terminal from a push server, comprising

the push server sends, in response to predetermined trigger events, at any time application push messages to a push client in the mobile terminal,

the push client in the wireless terminal detects connection availability of a device with a preferable alternative network connection, or the device with a preferable connection detects connection availability of the wireless terminal,

the push client is responsive to receipt of the application push message to push commands to an application in said device with a larger screen so as to bring forward view an application view identified by, modified by, contained in or otherwise affected in presentation by the received application push message.

31. A method of routing messages to a wireless terminal from a push server, comprising

the push server sends, in response to predetermined trigger events, at any time application push messages to a push client in the mobile terminal,

a push client in the wireless terminal detects a device with a preferred alternative network connection, or a push client in the device with a network connection detects physical proximity of the wireless terminal,

establishing a data-transfer capability between the push clients,
routing communication to and from the push client in the wireless terminal through the push client and the network connection of the device.

32. A method as claimed in any one of claims 1-31 wherein the push client accepts compressed information and optionally decompresses such information for the mobile application.

33. A method as claimed in any one of claims 1-32, wherein the push client and push server establish a secure connection and unwrap such security on behalf of the mobile application.

34. A server comprising means for performing the server steps as claimed in any one of method claims 1-33.

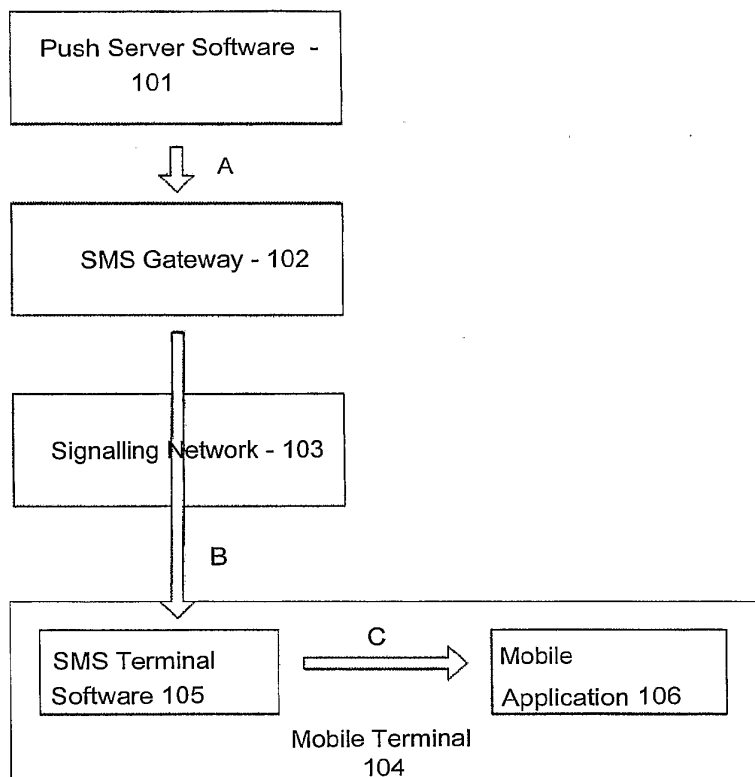
35. A wireless terminal comprising means for performing the push client steps as claimed in any one of method claims 1-34.

36. A program product comprising program code means which, when run in a computing unit of a wireless terminal, performs the push client steps as claimed in any one of method claims 1-35.

37. A program product comprising program code means which, when run in a computing device, performs the push server steps as claimed in any one of method claims 1-37.

1/15

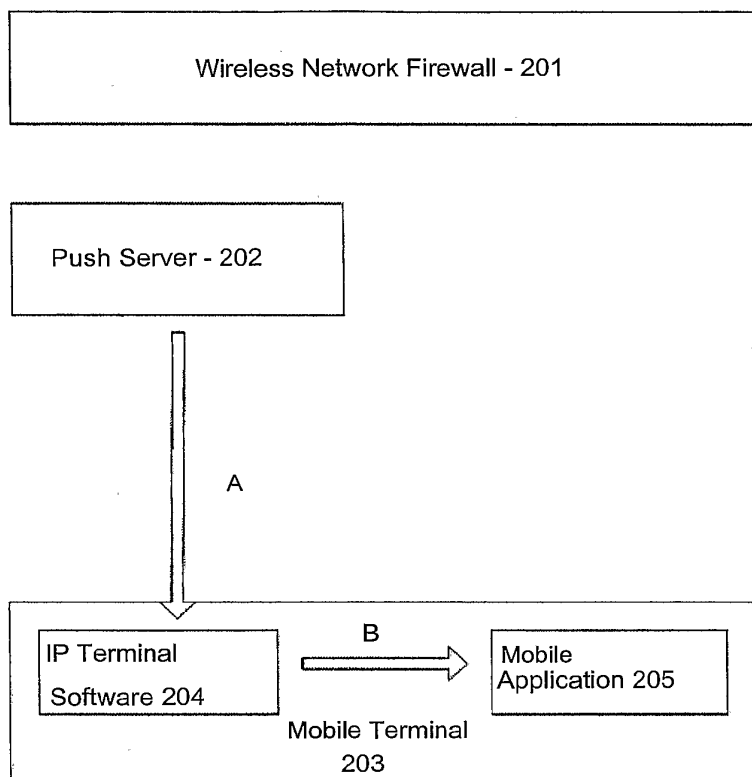
Figure 1



SUBSTITUTE SHEET (RULE 26)

2/15

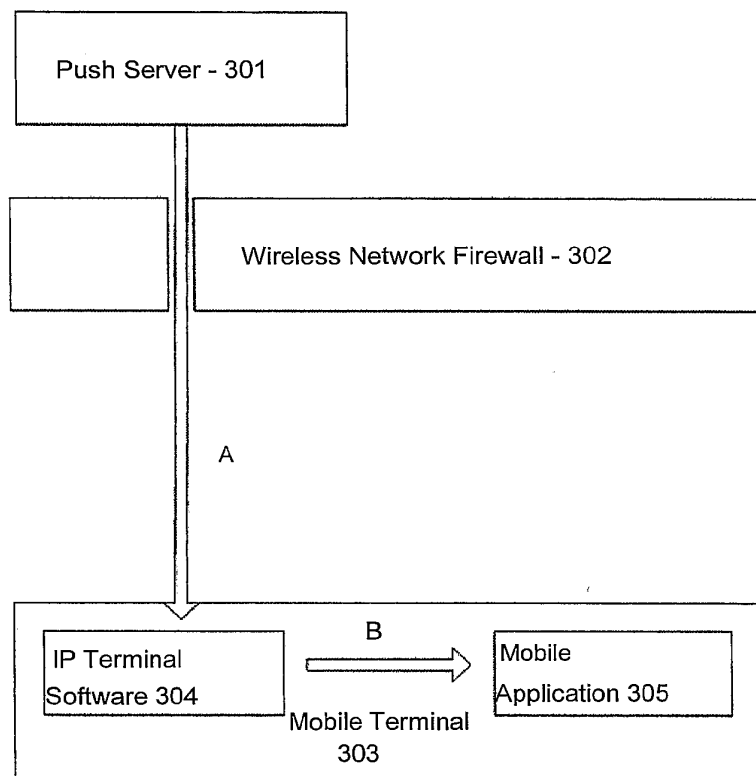
Figure 2



SUBSTITUTE SHEET (RULE 26)

3/15

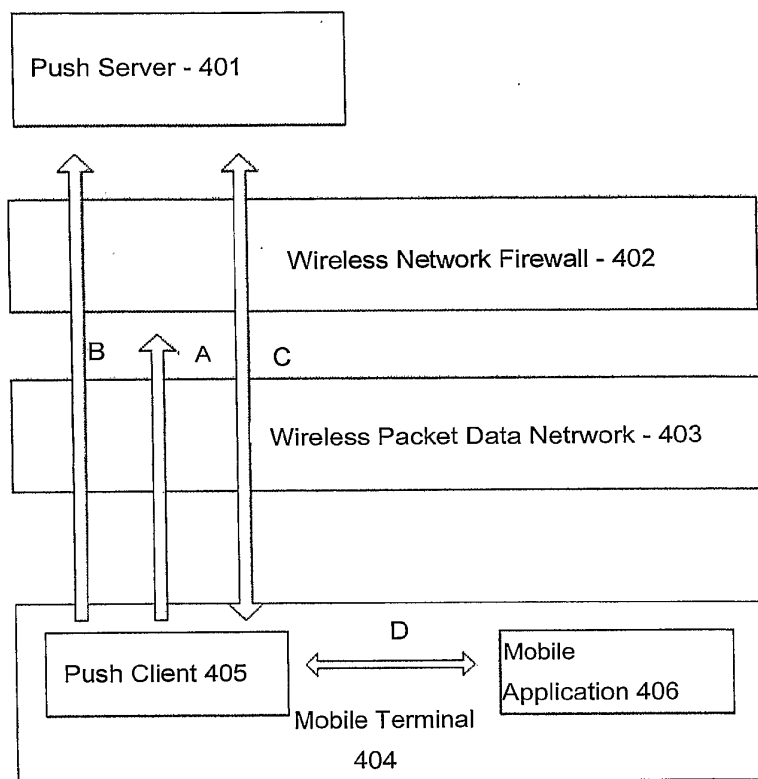
Figure 3



SUBSTITUTE SHEET (RULE 26)

4/15

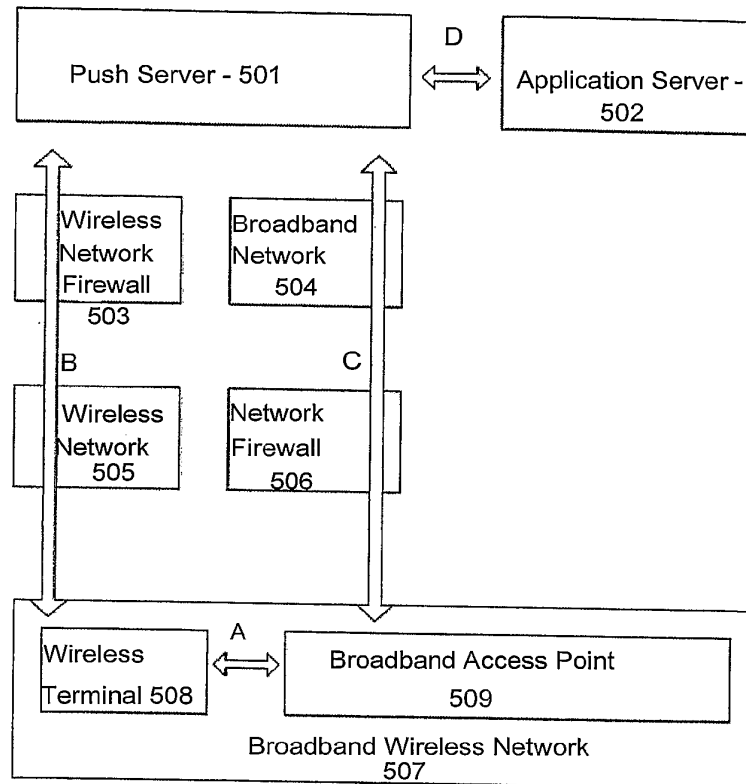
Figure 4



SUBSTITUTE SHEET (RULE 26)

5/15

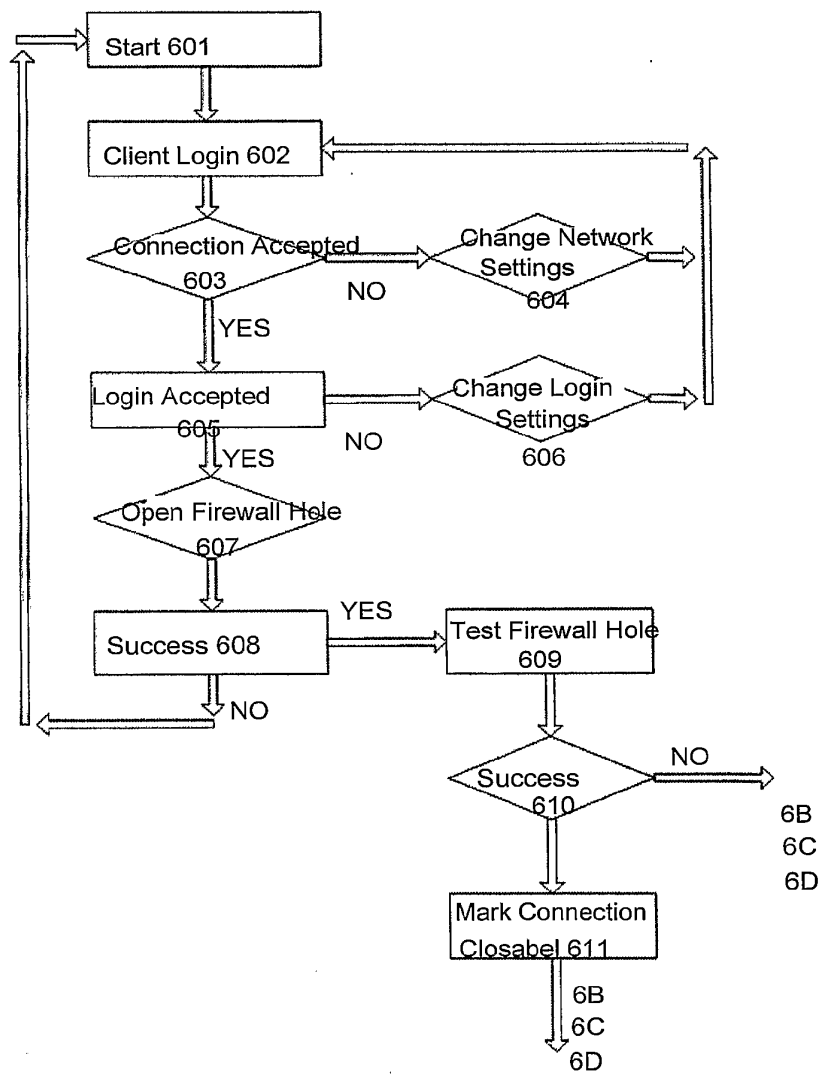
Figure 5



SUBSTITUTE SHEET (RULE 26)

6/15

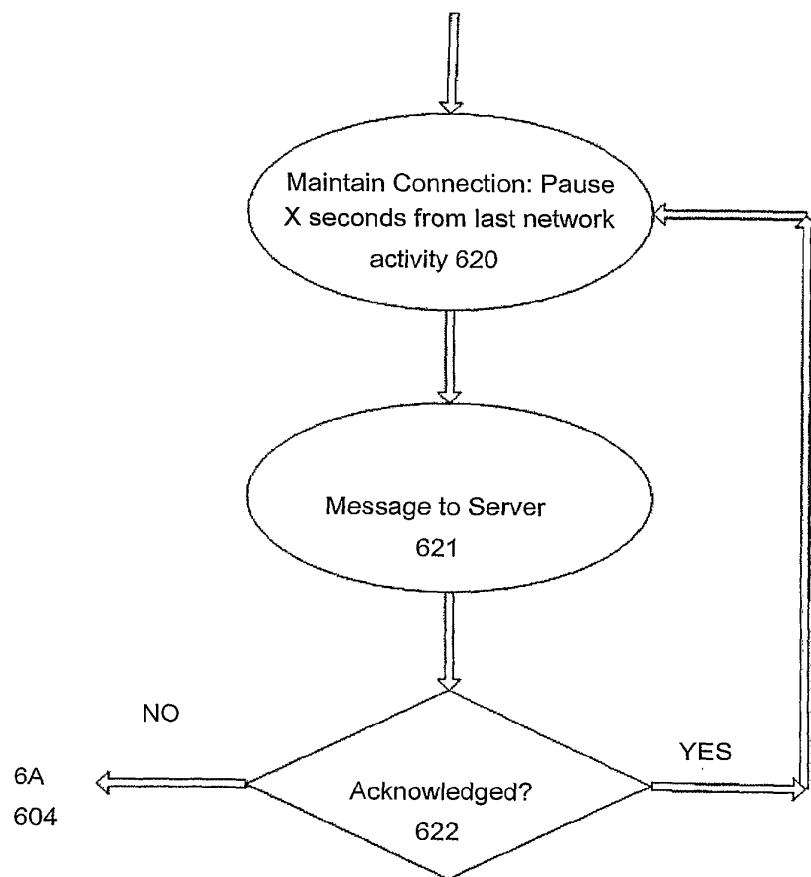
Figure 6A



SUBSTITUTE SHEET (RULE 26)

7/15

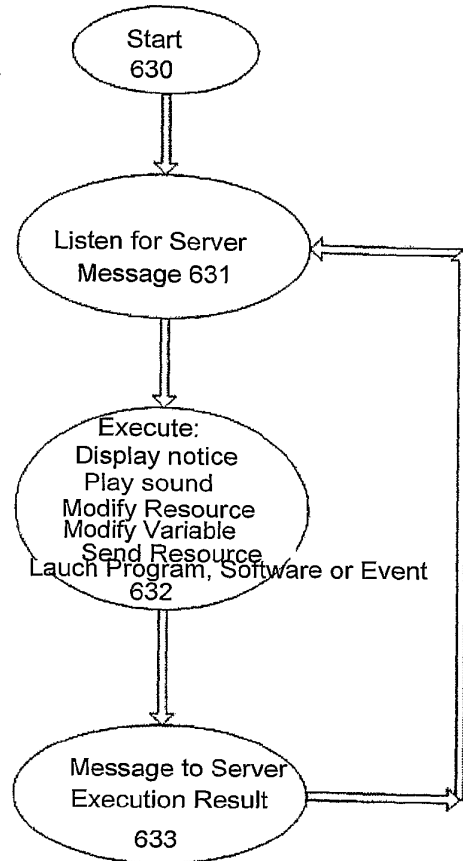
Figure 6B



SUBSTITUTE SHEET (RULE 26)

8/15

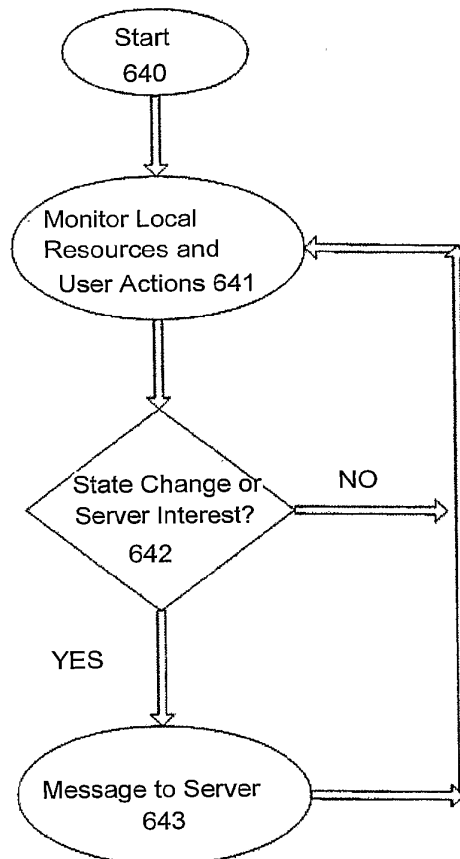
Figure 6C



SUBSTITUTE SHEET (RULE 26)

9/15

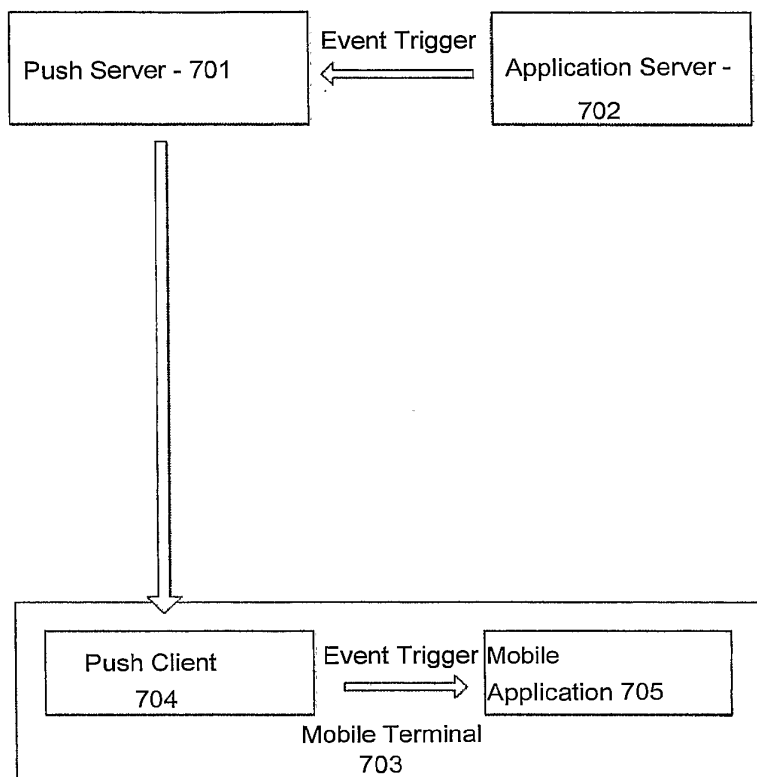
Figure 6D



SUBSTITUTE SHEET (RULE 26)

10/15

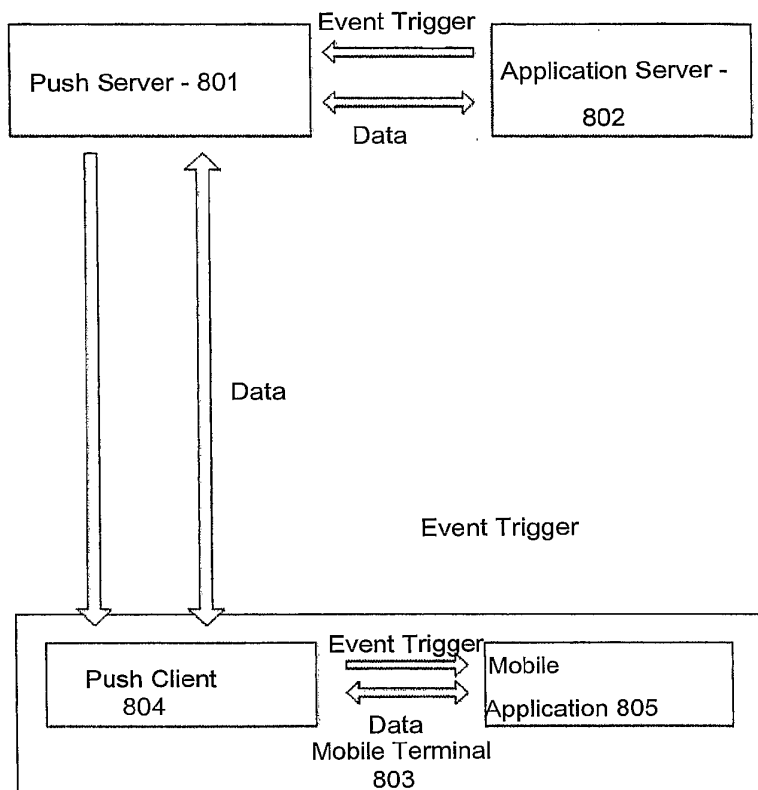
Figure 7



SUBSTITUTE SHEET (RULE 26)

11/15

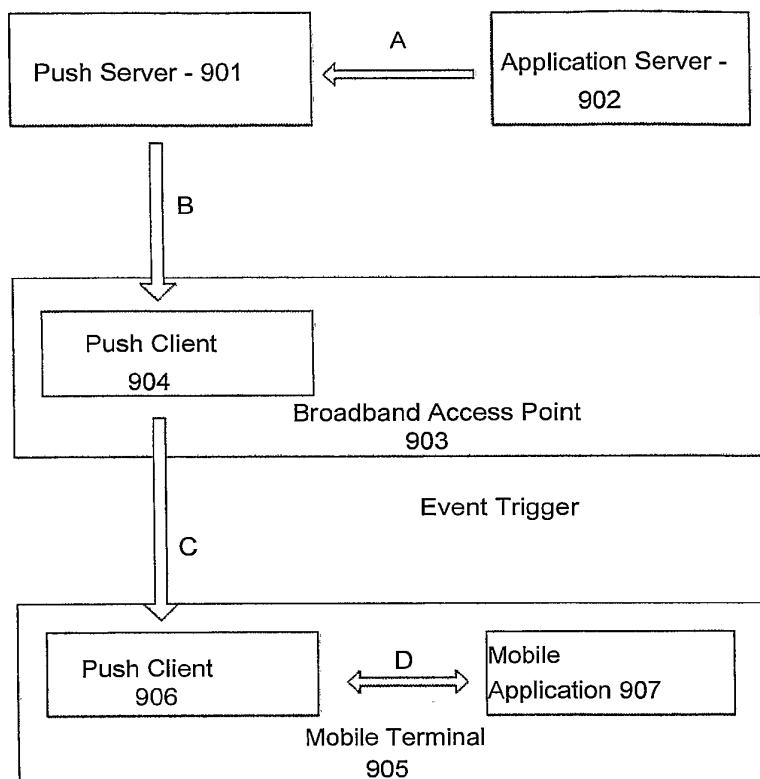
Figure 8



SUBSTITUTE SHEET (RULE 26)

12/15

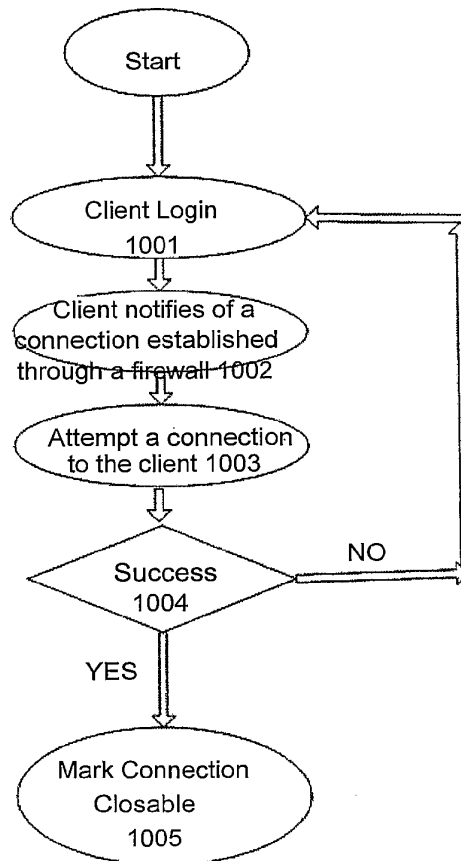
Figure 9



SUBSTITUTE SHEET (RULE 26)

13/15

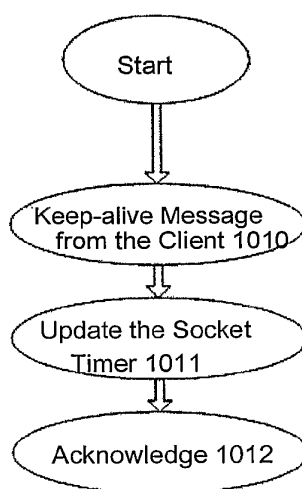
Figure 10A



SUBSTITUTE SHEET (RULE 26)

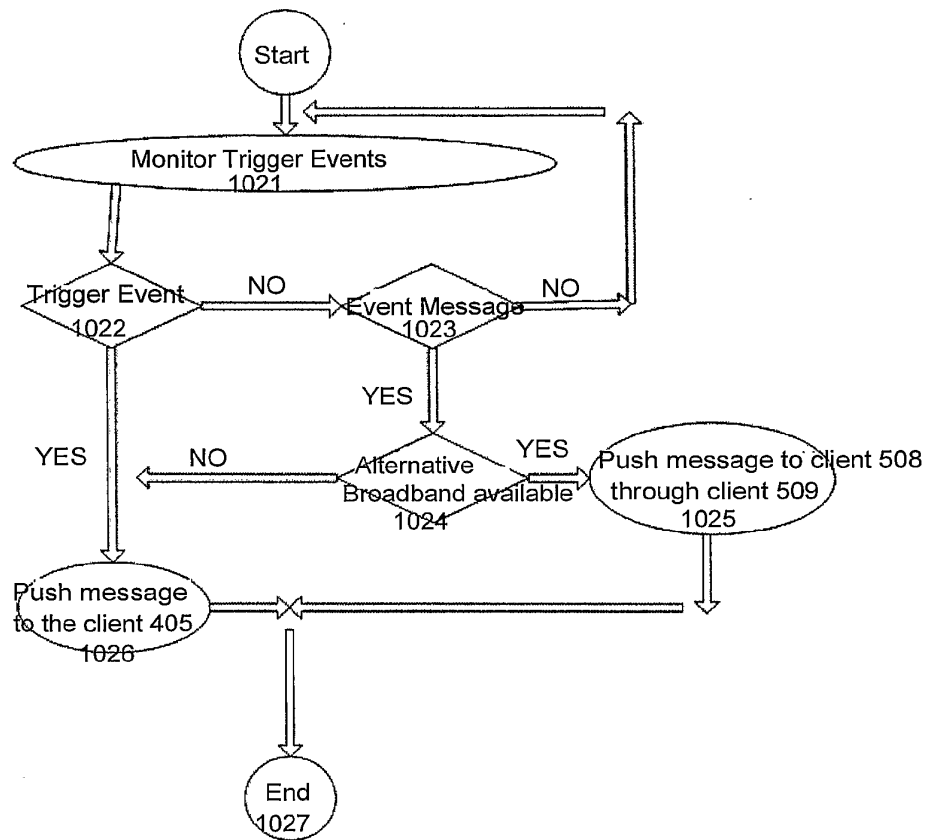
14/15

Figure 10B



SUBSTITUTE SHEET (RULE 26)

Figure 10C



INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI2006/050032

A. CLASSIFICATION OF SUBJECT MATTER		
See extra sheet		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC8: H04L, H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
FI, SE, NO, DK		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
EPO-INTERNAL, WPI, PAJ, INSPEC, IEEE Xplore		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2001/0005864 A1 (MOUSSEAU et al.) 28 June 2001 (28.06.2001), Abstract, paragraphs [0003], [0013], [0018], [0071], [0073], [0075]-[0082], fig. 6-9	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
Y	US 2003/0009561 A1 (SOLLEE) 09 January 2003 (09.01.2003), paragraphs [0007], [0027], [0076]	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
Y	WO 02067538 A2 (CELLTICK TECHNOLOGIES LTD et al.) 29 August 2002 (29.08.2002), Abstract, claim 6	1-4, 6-7, 13, 21-22, 28, 30-31, 34-37
A	JP 2003134566 A (AICON KK et al.) 09 May 2003 (09.05.2003), Abstract	1-37
A, P	US 2006/0009198 A1 (KASAI et al.) 12 January 2006 (12.01.2006), whole document	1-37
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
28 March 2006 (28.03.2006)		10 April 2006 (10.04.2006)
Name and mailing address of the ISA/FI National Board of Patents and Registration of Finland P.O. Box 1160, FI-00101 HELSINKI, Finland Facsimile No. +358 9 6939 5328		Authorized officer Seppo Ojala Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050032

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2001/0005864 A1	28/06/2001	US 2005148356 A1	07/07/2005
		JP 2005100427 A	14/04/2005
		JP 2005100426 A	14/04/2005
		JP 2005056437 A	03/03/2005
		US 2004252727 A1	16/12/2004
		JP 2004220622 A	05/08/2004
		US 2004073619 A1	15/04/2004
		US 2004024824 A1	05/02/2004
		US 2003187938 A1	02/10/2003
		US 2003050987 A1	13/03/2003
		US 2003005066 A1	02/01/2003
		US 2003018816 A1	23/01/2003
		US 2002194285 A1	19/12/2002
		US 2002049818 A1	25/04/2002
		US 2002029258 A1	07/03/2002
		EP 1282957 A2	12/02/2003
		EP 1273136 A2	08/01/2003
		EP 1273135 A2	08/01/2003
		CN 1436413 A	13/08/2003
		WO 0178342 A2	18/10/2001
		WO 0178341 A2	18/10/2001
		WO 0178319 A2	18/10/2001
		CA 2343932 A1	10/10/2001
		CA 2343905 A1	10/10/2001
		CA 2343648 A1	10/10/2001
		AU 5206001 A	23/10/2001
		AU 5020401 A	23/10/2001
		AU 5020101 A	23/10/2001
		US 2001054115 A1	20/12/2001
		US 2002120696 A1	29/08/2002
		US 2001005857 A1	28/06/2001
		US 2001005861 A1	28/06/2001
		US 2001004744 A1	21/06/2001
		US 2001005860 A1	28/06/2001
		US 2001013071 A1	09/08/2001
		US 2001009015 A1	19/07/2001
		MX PA00011592 A	17/10/2002
		NO 20005917 A	26/01/2001
		US 6463463 B1	08/10/2002
		US 6779019 B1	17/08/2004
		US 6463464 B1	08/10/2002
		US 6701378 B1	02/03/2004
		NZ 528050 A	28/01/2005
		NZ 508305 A	30/04/2004
		JP 2002517947T T	18/06/2002
		EP 1082839 A2	14/03/2001
		EP 1320221 A2	18/06/2003
		EP 1315336 A1	28/05/2003

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FI2006/050032

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
		EP 1206073 A2	15/05/2002
		EP 1126662 A2	22/08/2001
		EP 1124352 A2	16/08/2001
		EP 1098481 A2	09/05/2001
		EP 1096727 A2	02/05/2001
		EP 1096726 A2	02/05/2001
		EP 1096725 A2	02/05/2001
		CN 1304608 A	18/07/2001
		WO 9963709 A2	09/12/1999
		CA 2333881 A1	09/12/1999
		AU 3924499 A	20/12/1999
		AU 758302B B2	20/03/2003
		CA 2511594 A1	29/11/1999
		CA 2367135 A1	29/11/1999
		CA 2356324 A1	29/11/1999
		CA 2356073 A1	29/11/1999
		CA 2356046 A1	29/11/1999
		CA 2356038 A1	29/11/1999
		CA 2356004 A1	29/11/1999
		CA 2245157 A1	29/11/1999
		US 6219694 B1	17/04/2001
.....			
US 2003/0009561 A1	09/01/2003	WO 02103981 A2	27/12/2002
		EP 1446929 A2	18/08/2004
.....			
WO 02067538 A2	29/08/2002	RU 2004116910 A	10/10/2005
		US 2004078427 A1	22/04/2004
		EP 1362491 A2	19/11/2003
		CN 1493165 A	28/04/2004
.....			
JP 2003134566 A	09/05/2003	None	
.....			
US 2006/0009198 A1	12/01/2006	JP 2005108012 A	21/04/2005
.....			

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2006/050032

CLASSIFICATION OF SUBJECT MATTER

Int.Cl.

H04L 12/56 (2006.01)

H04L 29/08 (2006.01)

H04Q 7/22 (2006.01)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
24 April 2008 (24.04.2008)

PCT

(10) International Publication Number
WO 2008/048075 A1

(51) International Patent Classification:
H04Q 7/24 (2006.01)

(74) Agent: JIMYUNG Patent Firm; 6F, Jungwoo Bldg.,
1689-1, Seocho-4-dong, Seocho-gu, Seoul 137-882 (KR).

(21) International Application Number:
PCT/KR2007/005155

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date: 19 October 2007 (19.10.2007)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2006-0101714 19 October 2006 (19.10.2006) KR

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

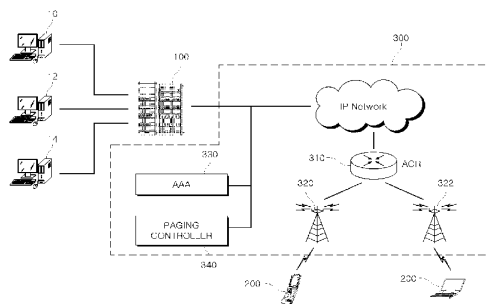
(71) Applicant (*for all designated States except US*): **INTRO MOBILE CO., LTD.** [KR/KR]; 2502-Ho, ASEM Tower, 159, Samseong-dong, Gangnam-gu, Seoul 135-798 (KR).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **LEE, Changseok** [KR/KR]; LG Apt. 101-1602, 12-2, Gaepo-dong, Gangnam-gu, Seoul 135-939 (KR).

Published:
— with international search report

(54) Title: SYSTEM OF PROVIDING INTEGRATED PUSH SERVICE AND METHOD THEROF



(57) Abstract: The present invention relates to a system and a method for providing an integrated push service in an internet service network, and the integrated push service system comprises a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data; an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push; a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information, wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.

WO 2008/048075 A1

Description

SYSTEM OF PROVIDING INTEGRATED PUSH SERVICE AND METHOD THEREOF

Technical Field

- [1] The present invention relates to a system and a method for providing an integrated push service in a network including a mobile internet such as Wibro.

Background Art

- [2] A mobile internet service such as a data service such as WAP (Wireless Application Protocol) based on a mobile communication network such as CDMA2000 1X, 3X, EV-DO, GSM and WCDMA, Wibro (Wireless Broadband) and HPi (High Speed Portable internet) are used to provide a data communication service such as the Internet through a mobile terminal. However, because the mobile communication network is mainly for a voice call and has complex network structure, a cost for building the mobile communication network is high. Therefore, a price per packet is excessive and the mobile communication network is not suitable for the Internet service based on a large capacity multimedia. The mobile internet service is to solve above-described problem wherein a conventional IP network is used to a maximum and a network structure is simple concentrating on a transmission of an IP packet. Therefore, the cost for building the network is low and the price per packet is low. Accordingly, an MBMM (Multiband Multimode) terminal using a conventional CDMA mobile communication modem for the voice call and the mobile internet such as Wibro for a data communication is used.
- [3] On the other hand, a push service is widely used for a sophisticated communication service. The push service actively transmits a data to a client by a server without a user intervention. For instance, an information selected by a user (a news, a stock information and a sports information) is provided to a user terminal in real time or a data for an upgrade is automatically transmitted to the user terminal in order to increase a user convenience.
- [4] However, when the push service is provided via the mobile internet network, problems described below occur.
- [5] First, since a push application server and a push application client should be built for each of the push services, an integrated operation of the network is difficult and a traffic increasing rapidly due to the push service is difficult to manage. In addition, in order to receive the push service in real time, the mobile terminal should load an application or an agent program for each of the push services in a memory. Therefore, a system efficiency is degraded due to a characteristic of the mobile terminal having

limited memory capacity, data processing capacity and battery capacity.

- [6] Second, the mobile terminal enters an idle mode when a data is not transceived considering a mobility of the mobile terminal in case of the mobile internet. In the idle mode, a generation of an unnecessary hand-over traffic is eliminated when moving between base stations in order to minimize a power consumption of the mobile terminal and enable an efficient use of a base station resources. However, in the idle mode, a push data cannot be transmitted to the mobile terminal in real time because the data is not transceived and a connection to a RAS (Radio Access Station) is disengaged.
- [7] Third, since the RAS used in the mobile internet service has a small service coverage compared to a mobile communication base station, a radio frequency shadow area is relatively large and the push data cannot be transmitted in real time when the mobile terminal in the shadow area.

Disclosure of Invention

Technical Problem

- [8] It is an object of the present invention to provide a system and a method for providing an integrated push service wherein various push data generated from a plurality of push application servers are transmitted through an integrated push service server and a mobile terminal extracts an associated application ID app_ID and loads an integrated push service agent selectively invoking a corresponding application to provide the various push services through a mobile internet network, and wherein a separate module for a transmission of the push data is not required for the push service server to reduce a cost for building the push service server, and wherein only a single integrated push service agent is loaded in a memory of the mobile terminal to optimize a system resource of the mobile terminal.
- [9] It is another object of the present invention to provide a system and a method for providing an integrated push service wherein an integrated push service server determines whether a receiving mobile terminal is in an idle mode and a push information is broadcasted via a paging controller provided by a mobile internet service network when the mobile terminal is in the idle mode to provide the push information in real time even to the mobile terminal having a communication session with the integrated push service server terminated in the idle mode.
- [10] It is yet another object of the present invention to provide a system and a method for providing an integrated push service wherein an integrated push service server transmits a push service as an SMS via a mobile communication service network instead of a mobile internet network when a receiving mobile terminal is not connected to the mobile internet network to provide the push information in real time even when

the mobile terminal of a user is in a shadow area of a mobile internet service.

Technical Solution

[11] In order to achieve above-described object, there is provided an integrated push service system comprising: a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data; an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push; a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information, wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.

[12] There is also provided a method for providing an integrated push service comprising steps of: (a) transmitting a push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data and an associated application ID specifying the application for invoking the push data to an integrated push service server through a communication network; (b) transmitting the push information to the receiving mobile terminal via an IP push through a mobile internet service network using the integrated push service server; and (c) receiving the push information using an integrated push service agent resident in a memory of the mobile terminal, and invoking the application compliant to the associated application ID to deliver the push data.

Advantageous Effects

[13] In accordance with the system and the method for providing the integrated push service of the present invention, the various push data generated from the plurality of push application servers are transmitted through the integrated push service server and the mobile terminal extracts the associated application ID app_ID and loads the

integrated push service agent selectively invoking the corresponding application to provide the various push services through the mobile internet network, the separate module for the transmission of the push data is not required for the push service server to reduce the cost for building the push service server, and only the single integrated push service agent is loaded in the memory of the mobile terminal to optimize the system resource of the mobile terminal.

[14] In accordance with the system and the method for providing the integrated push service of the present invention, the integrated push service server determines whether the receiving mobile terminal is in the idle mode and the push information is broadcasted via the paging controller provided by the mobile internet service network when the mobile terminal is in the idle mode to provide the push information in real time even to the mobile terminal having the communication session with the integrated push service server terminated in the idle mode.

[15] In accordance with the system and the method for providing the integrated push service wherein the integrated push service server transmits the push service as the SMS via the mobile communication service network instead of the mobile internet network when the receiving mobile terminal is not connected to the mobile internet network to provide the push information in real time even when the mobile terminal of the user is in the shadow area of the mobile internet service.

Brief Description of the Drawings

[16] Fig. 1 is a diagram illustrating a configuration of an integrated push service system in accordance with an embodiment of the present invention.

[17] Fig. 2 is a diagram illustrating a configuration of an integrated push service server in accordance with an embodiment of the present invention.

[18] Fig. 3 is a diagram illustrating a configuration of an integrated push service agent in accordance with an embodiment of the present invention.

[19] Fig. 4 is a diagram illustrating a hierarchy of an integrated push service agent in accordance with an embodiment of the present invention.

[20] Fig. 5 is a diagram illustrating a configuration of an integrated push service agent in accordance with an embodiment of the present invention.

[21] Figs. 6 through 8 are diagrams illustrating a communication system of a method for providing an integrated push service in accordance with an embodiment of the present invention.

Mode for the Invention

[22] Fig. 1 is a diagram illustrating a configuration of an integrated push service system in accordance with an embodiment of the present invention. Referring to Fig. 1, the integrated push service system comprises a plurality of push application servers 10, 12

and 14, an integrated push service server 100, a mobile internet service network 300, and a mobile terminal 200 including an integrated push service agent 250. The plurality of push application servers 10, 12 and 14 provides a push data to a push service application stored in the mobile terminal 200. The plurality of push application servers 10, 12 and 14 generate the push data push_data such as a real time news data for a news application, a chatting message for a peer-to-peer messenger application and an e-mail message for an e-mail application. A push information push_info including a receiving mobile terminal information specifying the mobile terminal that receives the push data, and an associated application ID app_ID specifying the application for invoking the push data along with the push data is also generated.

[23] In accordance with a conventional push application server, the associated application ID app_ID is not required because the conventional push application server is built for a single push application and a communication session and a protocol are maintained for each of the servers. However, in accordance with the present invention, various push services provided to each of applications are managed in an integrated fashion through the integrated push service server 100 and the integrated push service agent 250. Therefore, the associated application ID app_ID specifying the application for invoking the push data is required.

[24] <Transmission of the push information through an IP push>

[25] The integrated push service server 100 receives the push information push_info from the plurality of push application servers 10, 12 and 14 connected through a communication network, and provides the push information push_info to the mobile terminal 200 through an IP push push_IP. Because the mobile terminal 200 maintains a communication session with the integrated push service server 100 through a CSM (Communication Session Manager) 251 of the integrated push service agent 250, the push information push_info including the push data may be transmitted through the IP push push_IP. When the push information push_info is transmitted through the IP push push_IP, the integrated push service server 100 requests the IP push to the mobile internet service network 300.

[26] The mobile terminal 200 transmits a push information acknowledge message ack_push to the integrated push service server 100 when the push information push_info is received. the integrated push service server 100 acknowledges a successful transmission of the push data by receiving the push information acknowledge message ack_push at a reception acknowledge unit 142. A transmission report manager 140 transmits an information on the reception and a push application service to each of the plurality of push application servers 10, 12 and 14 as a transmission report.

[27] The mobile internet service network 300 is a high speed wireless internet service

such as Wibro and HPI which carries out a communication between the integrated push service server 100 and the mobile terminal 200, transmission/reception of the IP push data push_IP.

[28] The mobile terminal 200 receives the push information push_info in a form of the IP push push_IP through a mobile internet modem 210 for connecting to the mobile internet service network 300, and includes at least one application 260 that is to be associated with the push information push_info. Particularly, the mobile terminal 200 includes the integrated push service agent 250. The integrated push service agent 250 includes the CSM 251 resident on a memory of the mobile terminal 200 that maintains the communication session with the integrated push service server 100 in a state that the mobile internet modem 210 is connected to the mobile internet service network 300, and selectively invokes the application 260 compliant to the associated application ID app_ID of the push information push_info to deliver the push data.

[29] When an entirety of the applications 260 supporting a plurality of push services such as a chatting service, a mail service, a news service and a stock service in the mobile terminal 200 are resident in the memory in order to correspond to individual IP push in accordance with conventional art, a system resources of the mobile terminal 200 may be overloaded to degrade a processing speed thereof and is wasted. However, as shown in Fig. 3, only the integrated push service agent 250 of the mobile terminal 200 is resident in the memory of the mobile terminal 200 with each of the applications 260 being inactive in accordance with the embodiment of the present invention while an IP push receiver 252 receives the push information push_info for the entirety of the applications in an integrated fashion and uses the associated application ID app_ID included in the push information push_info to selectively invoke the application 260 corresponding to the associated application ID app_ID, thereby reducing a number of the applications resident in the memory and a power consumption of the mobile terminal 200.

[30] <Transmission of push information via paging message>

[31] On the other hand, a mobile internet service generally supports a power saving mode in order to reduce power consumption in a mobile environment. The mobile terminal 200 typically updates to which RAS 320 of a plurality of RASs 320 and 322 through a constant communication and a hand-over with the RASs 320 and 322. However, an unnecessary power consumption occurs for the mobile terminal 200 that does not have a constant transmission/reception of a data in order to maintain the constant communication with the mobile internet service network 300 for the hand-over and a registration of the RAS. As a result, the unnecessary power consumption has a serious effect on a DBDM(dual-band dual-mode) terminal using both the mobile internet service network 300 and a mobile communication service network 400 such as

a CDMA and a GSM or MBMM(multi-band multi-mode) terminal supporting three or more communication services.

- [32] The power saving mode provided by the mobile internet service is to solve above-described problem. In the power saving mode, the mobile terminal 200 enters an idle mode wherein a connection to the RAS 320 is lost when an exchange of the data with a mobile internet network is not carried out for more than a predetermined time. The idle mode refers to a state that the transmission/reception of the data by the mobile terminal 200 is not carried out and the connection to the RAS 320 is lost to eliminate a generation of an unnecessary hand-over traffic between the mobile terminal 200 and the RASs 320 and 322, thereby minimizing the power consumption of the mobile terminal 200 and enabling an efficient use of the RASs 320 and 322.
- [33] When a packet to be transmitted to the mobile terminal 200 is generated in the idle mode, a paging controller 340 of the mobile internet service network 300 broadcasts a paging message through the RASs 320 and 322 of a paging group consisting of the plurality of RASs wherein the mobile terminal 200 expected to exist. Through this process, the mobile terminal 200 receives a downlink data packet to exit the idle mode and enter a normal mode to re-connect to the mobile internet service network 300.
- [34] In accordance with the embodiment of the present invention, a push service may be provided continuously for the mobile terminal 200 in the idle mode by transmitting the push information through the paging message. When the mobile terminal 200 enters the idle mode, the CSM 251 of the integrated push service agent 250 of the mobile terminal 200 cannot send the push information push_info through the IP push push_IP because the communication session with the integrated push service server 100 is terminated. While the integrated push service server 100 may schedule and transmit the push information push_info or re-transmit the push information push_info by recognizing a communication configuration of the mobile terminal 200, the push service cannot be provided in real time.
- [35] It is preferable that the push information push_info is included in the paging message instead of the IP push push_IP such that the push service is provided to the mobile terminal 200 in real time in order to solve above-described problem.
- [36] There are two methods for the mobile terminal 200 to recognize the idle mode of the mobile terminal 200. In accordance with a first method, whether the mobile terminal 200 is in the idle mode is registered in a presence server 130 such that the integrated push service server 100 may inquire the presence server 130 of whether the mobile terminal 200 is in the idle mode prior to transmitting the push information push_info. In accordance with a second method, the integrated push service server 100 transmits the push information push_info by the IP push push_IP and determines that the mobile terminal 200 is in the idle mode when the push information acknowledge

message ack_push is not received from the mobile terminal 200.

- [37] While a configuration of the integrated push service server 100 is complex due to an association with the presence server 130, an unnecessary IP push is omitted to enable an efficient use of a network resource in accordance with the first method. While an unnecessary traffic is generated due to the IP push push_IP, the integrated push service server 100 does not require the association with the presence server 130, thereby simplifying a system configuration in accordance with the second method.
- [38] The first method wherein the presence server 130 is used is described below in detail.
- [39] In accordance with first method, the integrated push service server 100 or the mobile internet service network 300 further includes the presence server 130 that determines whether the mobile terminal 200 is in the idle mode, and also further comprises the paging controller 340 for broadcasting the paging message for the mobile terminal 200 through the at least one RASs 320 and 322. The integrated push service server 100 provides the push information push_info to the paging controller 340 when the mobile terminal 200 is determined to be in the idle mode using the presence server 130, and the integrated push service agent further comprises a paging message parser 253 for parsing the push information push_info when the push information push_info is received as the paging message push_paging.
- [40] In accordance with first method, the integrated push service server 100 inquires the presence server 130 of whether the mobile terminal 200 is in the idle mode and transmits the push information push_info as the paging message push_paging through the paging controller 340 instead of the IP push push_IP in the idle mode. The mobile terminal 200 extracts the push data push_data and the associated application ID app_ID from the paging message push_paging through the paging message parser 253 as the paging message push_paging is received. The corresponding application 260 is then invoked to provide various push services between the plurality of push application servers 10, 12 and 14 and the mobile terminal 200.
- [41] The second method wherein the presence server 130 is not used is described below in detail.
- [42] In accordance with second method, the integrated push service agent 250 further comprises a reception acknowledge report manager 256 for generating the push information acknowledge message ack_push, and the mobile internet service network 300 further comprises the paging controller 340 for broadcasting the paging message for the mobile terminal 200 through the at least one RASs 320 and 322. The integrated push service server 100 provides the push information push_info to the paging controller 340 when the push information acknowledge message ack_push is not received from the reception acknowledge report manager 256, and the mobile terminal

200 is configured to further include the paging message parser 253 for parsing for parsing the push information push_info when the push information push_info is received as the paging message push_paging.

[43] In accordance with second method, the integrated push service server 100 transmits the push information push_info via the IP push push_IP and determines that the mobile terminal 200 is in the idle mode when the push information acknowledge message ack_push is not received. The mobile terminal 200 extracts the push data push_data and the associated application ID app_ID from the paging message push_paging through the paging message parser 253 as the paging message push_paging is received. The corresponding application 260 is then invoked to provide various push services between the plurality of push application servers 10, 12 and 14 and the mobile terminal 200.

[44] In accordance with the embodiment wherein the push information push_info is transmitted through the paging message push_paging, it preferable that the CSM 251 of the integrated push service agent 250 of the mobile terminal 200 controls the mobile internet modem 210 to configure the communication session between the integrated push service server 100 and the integrated push service agent 250. In case that the push data push_data is too large to be transmitted efficiently by only the paging message push_paging or that other data is to be transmitted after the transmission of the push information push_info, the mobile terminal 200 automatically exits the idle mode to configure the communication session with the integrated push service server 100 when the push information push_info is received as the paging message push_paging, thereby efficiently providing the push service.

[45] <Transmission of push information through SMS of service network>

[46] Since the mobile internet service is designed for a data communication, the mobile internet service is disadvantageous over the mobile communication service such as CDMA and GSM. Considering the disadvantage, a DBDM terminal or a MBMM terminal supporting both the mobile communication service and the mobile internet service is used. In such case, the mobile terminal 200 includes the mobile internet modem 210 and a mobile communication modem 220.

[47] However, in accordance with embodiment, while the mobile internet modem 210 maintains the communication with the mobile communication service network 400 in order to receive an incoming call, a communication with the mobile internet service network 300 for the data communication is established selectively when required by a user. In addition, since the mobile internet service network 300 has a small service coverage compared to the mobile communication service network 400, the communication with the mobile communication service network 400 is frequently terminated when the mobile terminal 200 enters a shadow area.

- [48] When the mobile terminal 200 is unable to establish the communication with the mobile communication service network 400, the push data push_data cannot be transmitted via the IP push push_IP or the paging message push_paging even when a new push data push_data is generated in a push application server 10.
- [49] In such case, the integrated push service agent 250 connects to the paging controller 340 and informs the integrated push service server 100 of the mobile terminal 200 entering the network once connected to the mobile internet service network 300. the integrated push service server 100 searches whether the push information push_info that is not transmitted to the mobile terminal 200 exists to transmit the push information push_info as the IP push push_IP or the paging message push_paging. However, the push service is not provided in real time even in accordance with the embodiment.
- [50] In order to solve above-described problem, the integrated push service system further comprises the mobile communication service network 400 including a plurality of base stations and a SMSC, the mobile terminal 200 further comprises the mobile communication modem 220 for connecting to the mobile communication service network 400, the integrated push service server 100 transmits the push information push_info to the SMSC of the mobile communication service network 400 when the mobile terminal 200 is determined to be disconnected from the mobile internet service network, and the integrated push service agent 250 further comprises an SMS parser 254 for parsing the push information push_info when the push information push_info is received via an SMS push_SMS through the mobile communication modem 250.
- [51] In accordance with the embodiment, a real time push service is possible since the push information push_info may be transmitted via the SMS push_SMS even when the mobile terminal 200 is not connected to the mobile internet service network 300.
- [52] On the other hand, in a certain case, the push data push_data should be transmitted to the application 260 using a data service provided by the mobile communication service network 400 such as WAP (wireless Application Protocol) instead of the application 260 using the mobile internet service network 300. Typically, a method wherein a connection to a data network of a corresponding mobile communication service via the SMS is used. In such case, the integrated push service agent 250 may be configured to further include a mobile communication service interface. The integrated push service agent 250 further comprises the mobile communication service interface for controlling the mobile communication modem 220 to connect to the data network provided by the mobile communication service network 400, and may be configured to control the mobile communication modem 220 to connect to the data network of the mobile communication service network when the associated application ID app_ID of the received push information push_info designates the application 260 associated with

the data network of the mobile communication service network 400.

- [53] <Method for providing integrated push service>
- [54] Figs. 6 through 8 are diagrams illustrating a communication system of a method for providing an integrated push service in accordance with an embodiment of the present invention.
- [55] First steps (S100 and S120) are carried out wherein a push information push_info including a push data push_data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data push_data and an associated application ID app_ID specifying the application for invoking the push data push_data is transmitted to an integrated push service server through a communication network.
- [56] Thereafter, second steps S200 and S210 are carried out wherein a integrated push service server 100 transmits the push information push_info to the receiving mobile terminal 200 via an IP push through a mobile internet service network 300.
- [57] Thereafter, third steps S500 and S600 are carried out wherein an integrated push service agent 250 resident in a memory of the mobile terminal 200 receives the push information push_info (S500) and invokes an application 260 compliant to the associated application ID app_ID to deliver the push data push_data.
- [58] The embodiment is described in detail wherein the push information push_info is transmitted as a paging message push_message in order to provide the integrated push service even when the mobile terminal 200 is in an idle mode.
- [59] First, the method for providing the integrated push service further comprises a fourth step wherein a presence server 130 detects the idle mode of the mobile terminal 200 prior to the first steps S100 and S120, the second steps S200 and S210 further comprises a first sub-step S305 wherein the push information push_info is requested to a paging controller 340 of the mobile internet service network 300 to be transmitted as the paging message push_paging when the mobile terminal 200 is determined to be in the idle mode, and a second sub-step S310 wherein the paging controller 340 broadcasts the push information push_info as the paging message push_paging through at least one RASs 320 and 211, and the third step S600 may be configured in a manner that the integrated push service agent 250 parses the paging message push_paging to extract the push information push_info.
- [60] In accordance with the embodiment shown in Fig. 7 wherein the presence server 130 is not used, the third step further comprises a third sub-step (S700) wherein the integrated push service agent 250 transmits a reception acknowledge message ack_push to the integrated push service server according to the reception of the push information push_info, the second steps S200 and S210 further comprises a first sub-step S305 of requesting a paging controller of the mobile internet service network to

transmit the push information push_info as the paging message push_paging when the reception acknowledge message is not received and a fifth sub-step S310 wherein the paging controller 340 broadcasts the push information push_info as the paging message push_paging through at least one RASs 320 and 322, and the third step S600 may be configured to in a manner that the integrated push service agent 250 parses the paging message push_paging to extract the push information push_info.

- [61] After carrying out the third step S600, the integrated push service agent 250 may further establish a communication session with the integrated push service server according to the reception of the push information push_info.
- [62] Finally, an embodiment of the method for providing the integrated push service using the SMS wherein the mobile terminal 200 is a DBDM terminal that may connect to the mobile internet service network 300 and the mobile communication service network 400 and the mobile terminal 200 is not connected to the mobile internet service network 300 to provide the integrated push service in real time is described below in detail.
- [63] As shown in Fig. 8, the second steps S200 and S210 comprises a sixth sub-step wherein the push information push_info is transmitted to an SMSC of the mobile communication service network 400 when the mobile terminal 200 is determined to be disconnected from the mobile internet service network 300 and a seventh sub-step wherein the SMSC transmits the push information push_info to the receiving mobile terminal 200 as the SMS push_SMS, and the third steps S500 and S600 further comprises an eighth sub-step wherein the integrated push service agent 250 parses the received SMS push_SMS to extract the push information push_info.
- [64] While the present invention has been particularly shown and described with reference to the preferred embodiment thereof, it will be understood by those skilled in the art that various changes in form and details may be effected therein without departing from the spirit and scope of the invention as defined by the appended claims.

Claims

- [1] An integrated push service system comprising:
a plurality of push application servers for providing a push information, the push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data, and an associated application ID specifying the application for invoking the push data;
an integrated push service server for receiving the push information and providing the push information to the mobile terminal receiving the push data through an IP push;
a mobile internet service network including a plurality of RASs to carry out a communication between the push service server and the mobile terminal receiving the push data; and
the mobile terminal for receiving the push information through a mobile internet modem for connecting to the mobile internet service network, the mobile terminal comprising at least one application for associating with the push information,
wherein the mobile terminal further comprises a communication session manager resident in a memory thereof, the communication session manager maintaining a communication session with the integrated push service server when the mobile internet modem is connected to the mobile internet service network, and an integrated push service agent for selectively invoking the application compliant to the associated application ID of the received push information to deliver the push data.
- [2] The system in accordance with claim 1, wherein the integrated push service server or the mobile internet service network further comprises a presence server for detecting an idle mode of the mobile terminal,
wherein the mobile internet service network further comprises a paging controller for broadcasting a paging message for the mobile terminal through the at least one RAS,
wherein the integrated push service server provides the push information to the paging controller when the mobile terminal is determined to be in the idle mode through the presence server, and
wherein the integrated push service agent further comprises a paging message parser for parsing the push information when the push information is received as the paging message.
- [3] The system in accordance with claim 1, wherein the integrated push service

agent further comprises a reception acknowledge report manager for generating a push information reception acknowledge message according to the reception of the push information,

wherein the mobile internet service network further comprises a paging controller for broadcasting a paging message for the mobile terminal through the at least one RAS,

wherein the integrated push service server provides the push information to the paging controller when the push information reception acknowledge message is not received from the reception acknowledge report manager after transmitting the push message via an IP push, and

wherein the mobile terminal further comprises a paging message parser for parsing the push information when the push information is received as the paging message.

[4] The system in accordance with one of claims 2 and 3, wherein the communication session manager establishes a communication session between the integrated push service server and the integrated push service agent by controlling the mobile internet modem when the push information is received as the paging message.

[5] The system in accordance with one of claims 2 and 3, wherein the integrated push service server stores the push information when the mobile terminal is not connected to the mobile internet service network and transmits the stored push information when the mobile terminal is connected to the mobile internet service network.

[6] The system in accordance with claim 5, wherein the integrated push service agent informs the integrated push service server of an entrance to the mobile internet service network via the paging message by connecting to the paging controller when connected to the mobile internet service network.

[7] The system in accordance with one of claims 1 through 3, further comprising a mobile communication service network including a plurality of base stations and a SMSC,

wherein the mobile terminal further comprises a mobile communication modem for connecting to the mobile communication service network,

wherein the integrated push service server transmits the push information to the SMSC of the mobile communication service network when the mobile terminal is determined to be disconnected from the mobile internet service network, and wherein the integrated push service agent further comprises an SMS parser for parsing the push information when the push information is received via an SMS through the mobile communication modem.

- [8] The system in accordance with claim 7, wherein the integrated push service agent the integrated push service agent further comprises a mobile communication service interface for controlling the mobile communication modem to connect to a data network provided by the mobile communication service network, and controls the mobile communication modem to connect to the data network of the mobile communication service network when the associated application ID of the received push information designates the application associated with the data network of the mobile communication service network.
- [9] The system in accordance with one of claims 1 through 3, wherein the integrated push service server further comprises a transmission report manager for generating a transmission report including a result of a push information transmission, and transmits the result of the push information transmission to the push application server providing the push information.
- [10] A method for providing an integrated push service comprising steps of:
(a) transmitting a push information including a push data invoked through an application of a mobile terminal, a receiving mobile terminal information specifying the mobile terminal receiving the push data and an associated application ID specifying the application for invoking the push data to an integrated push service server through a communication network;
(b) transmitting the push information to the receiving mobile terminal via an IP push through a mobile internet service network using the integrated push service server; and
(c) receiving the push information using an integrated push service agent resident in a memory of the mobile terminal, and invoking the application compliant to the associated application ID to deliver the push data.
- [11] The method in accordance with claim 10, further comprising (d) detecting an idle mode of the mobile terminal by a presence server prior to the step (a), wherein the step (b) further comprises:
(a-1) requesting the push information as a paging message using a paging controller of the mobile internet service network when the mobile terminal is determined to be in the idle mode; and
(a-2) broadcasting the push information as the paging message through at least one RAS using the paging controller, and
wherein the step (c) comprises extracting the push information by parsing the paging message using the integrated push service agent.
- [12] The method in accordance with claim 10, wherein the step (c) further comprises (c-1) transmitting a reception acknowledge message to the integrated push service server according to the reception of the push information using the

integrated push service agent,

wherein the step (b) further comprises:

(b-1) requesting a paging controller of the mobile internet service network to transmit the push information as the paging message when the reception acknowledgment message is not received; and

(b-2) broadcasting the push information as the paging message through at least one RAS using the paging controller, and

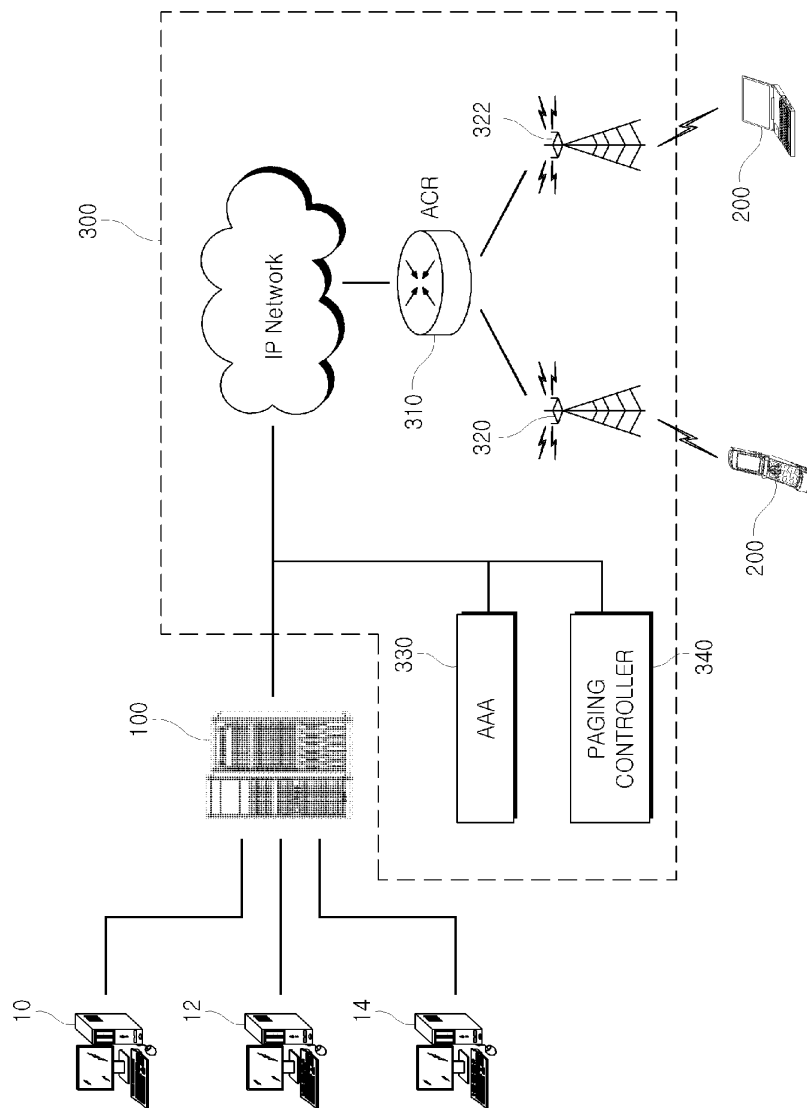
wherein the step (c) extracting the push information by parsing the paging message using the integrated push service agent.

[13] The method in accordance with one of claims 11 and 12, wherein further comprising (e) establishing a communication session between the integrated push service server and the integrated push service agent according to the reception of the push information after carrying out the step (c).

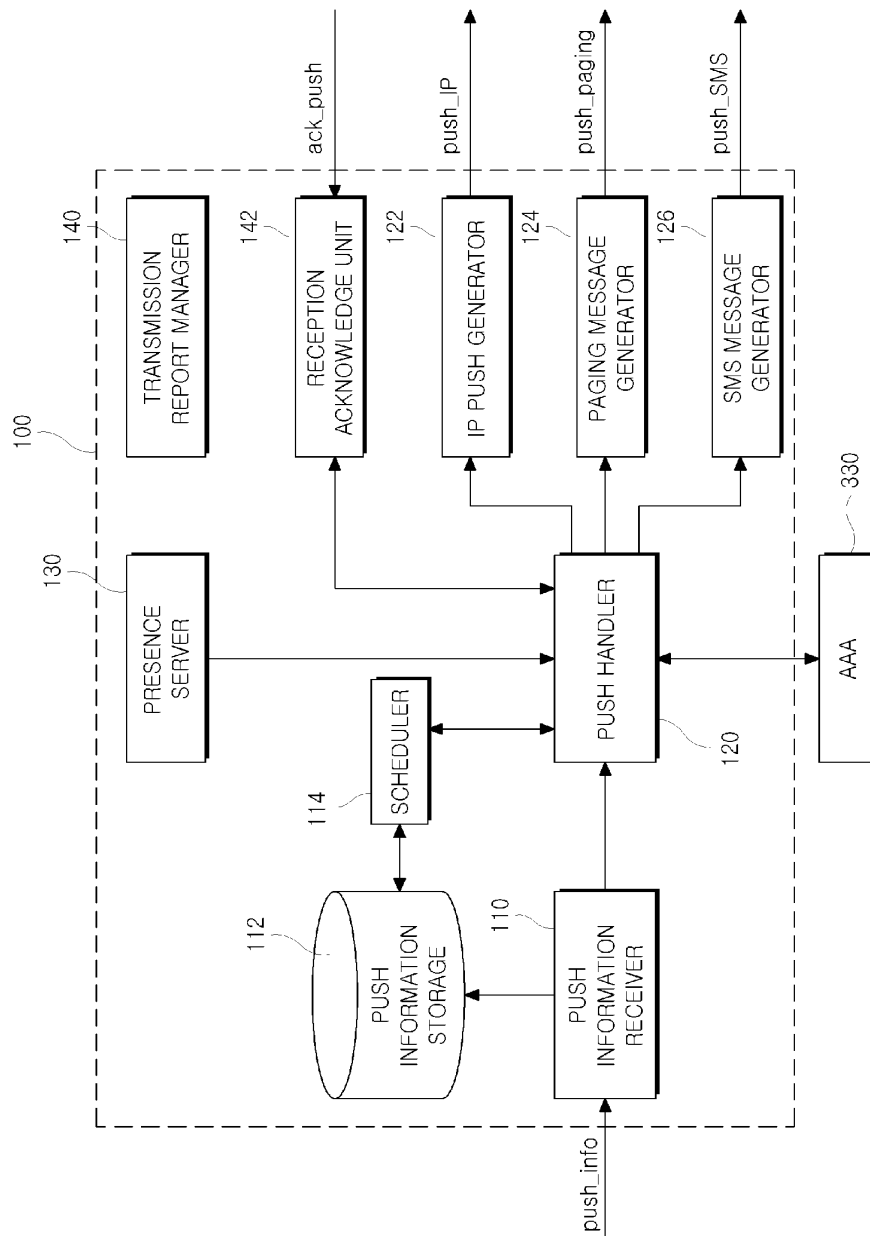
[14] The method in accordance with one of claims 11 and 12, wherein the step (b) comprises storing the push information when the mobile terminal is not connected to the mobile internet service network, and re-transmitting the stored push information when the mobile terminal is connected to the mobile internet service network.

[15] The method in accordance with one of claims 11 and 12, wherein the step (b) comprises:
(b-3) transmitting the push information to a SMSC of the mobile internet service network when the mobile terminal is determined to be disconnected from the mobile internet service network; and
(b-4) transmitting the push information to the receiving mobile terminal as an SMS by the SMCC, and
wherein the step (c) further comprises (c-2) extracting the push information by parsing the SMS by the integrated push service agent.

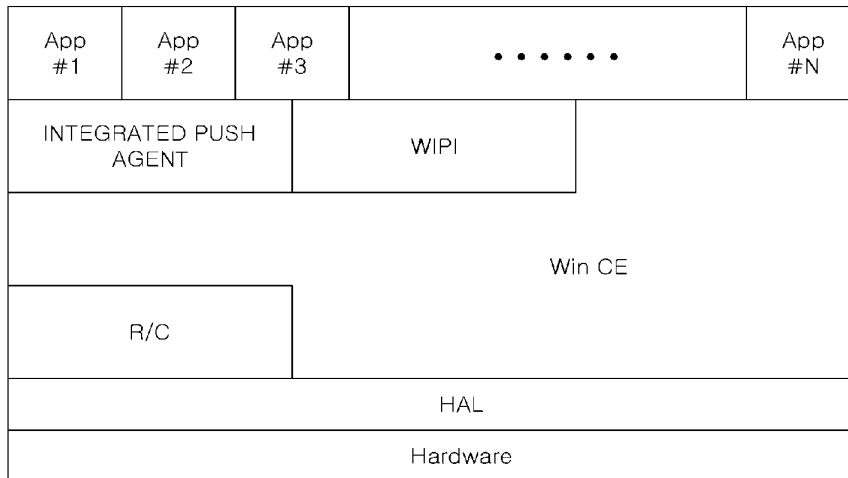
[Fig. 1]



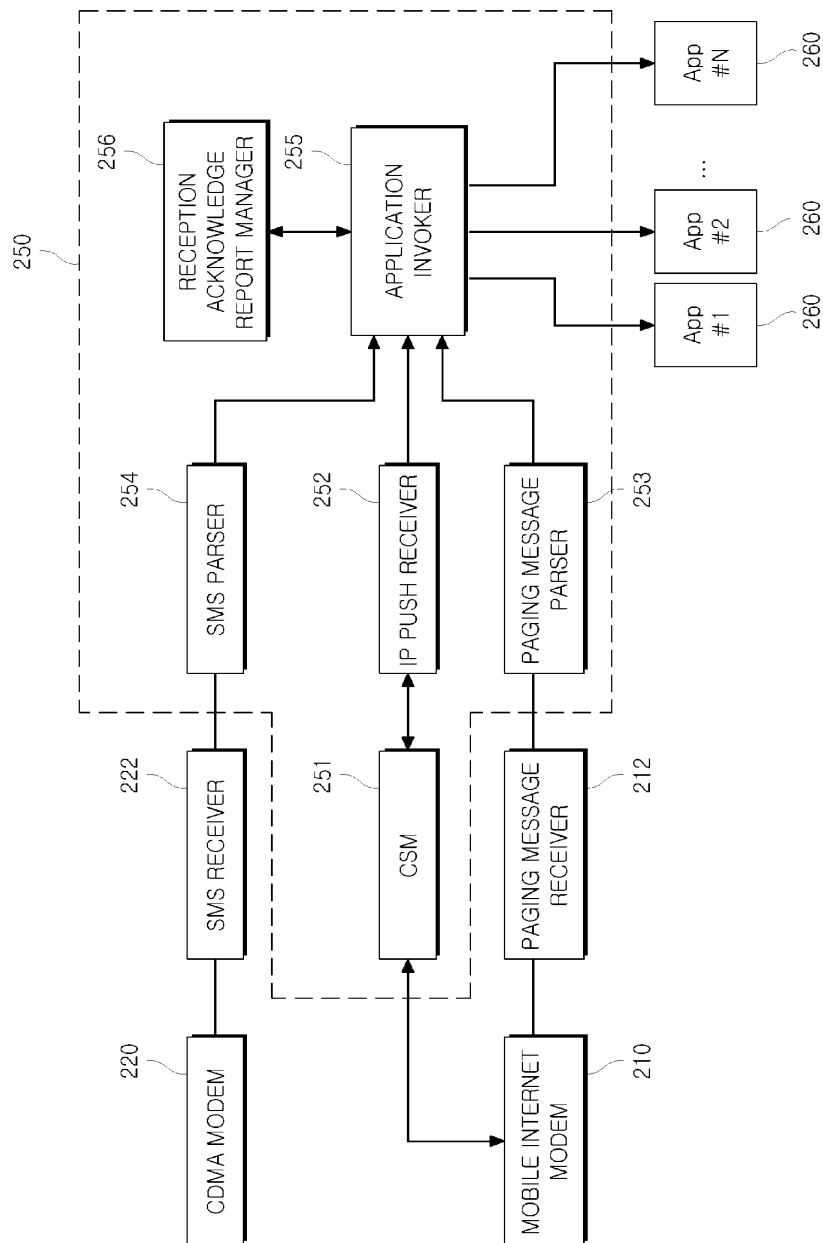
[Fig. 2]



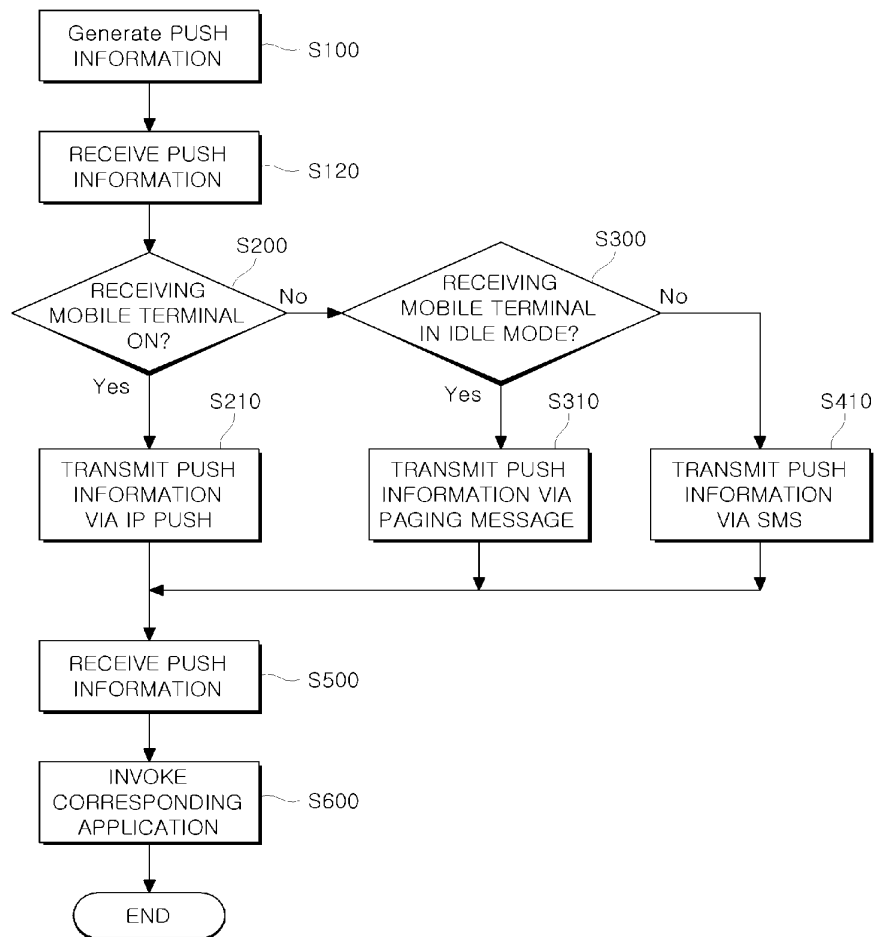
[Fig. 3]



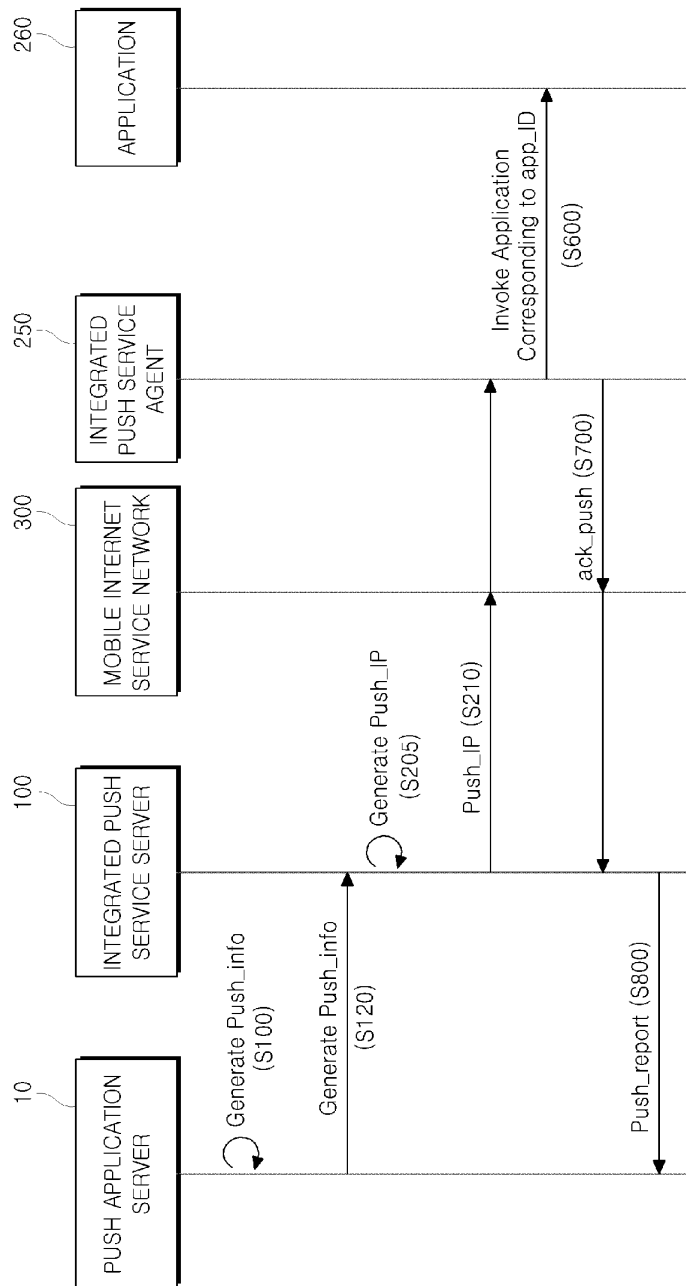
[Fig. 4]



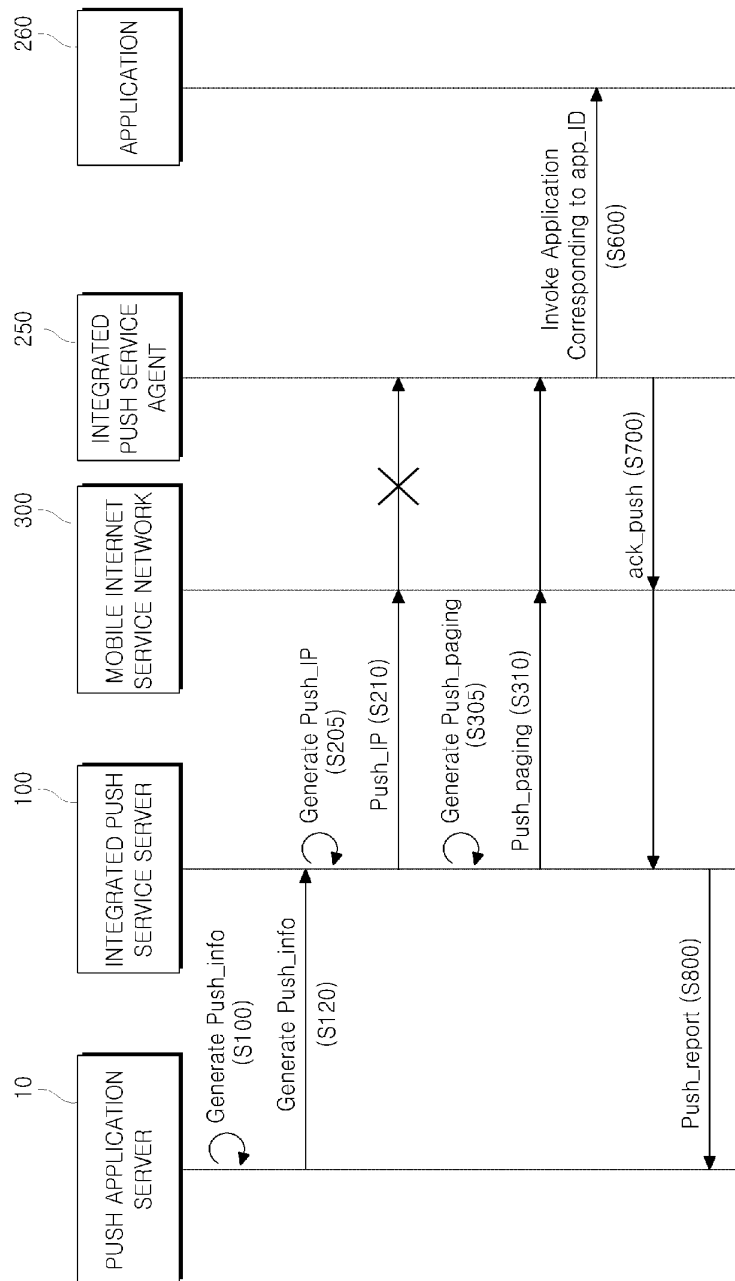
[Fig. 5]



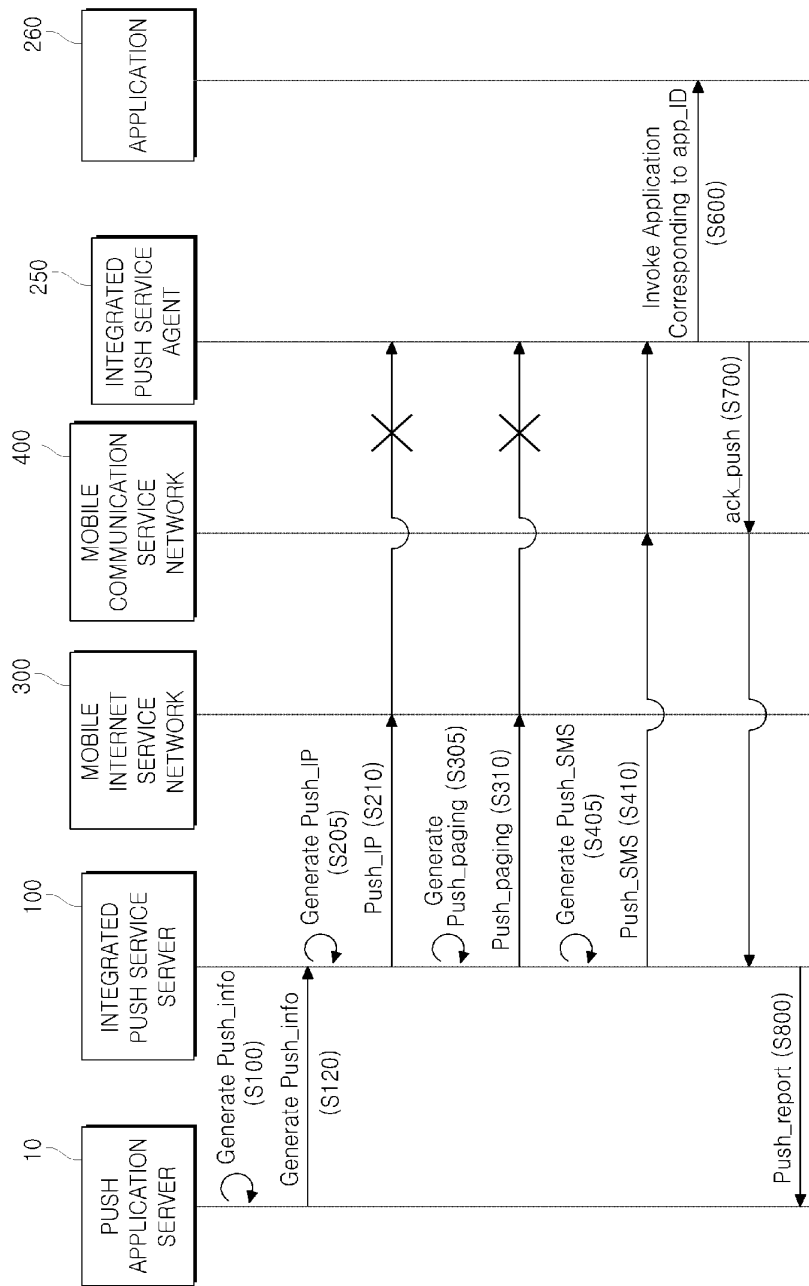
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2007/005155**A. CLASSIFICATION OF SUBJECT MATTER****H04Q 7/24(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : H04Q 7/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility Models since 1975

Japanese Utility models and applications for Utility Models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS(KIPO internal) "push, application, server, agent"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 06999991 B1 (Ikeda, H.) 14 Feb. 2006 See abstract, figures 1-2, claims 1-9, and column 6, line 53 - column 8, line 5	1-15
A	US 2002-0116472 A1 (Kalish, D. et al.) 22 Aug. 2002 See abstract, figures 1-2, claims 1-10, and paragraphs [0020]-[0032]	1-15
A	KR 10-2003-0037448 A (SK TELECOM CO., LTD.) 14 May 2003 See abstract, figure 2, claims 1-5, and page 3, lines 20-47	1-15
A	KR 10-2004-0045803 A (WIDERTHAN.COM CO., LTD.) 02 Jun. 2004 See abstract, figures 3-4, claims 1-4, and page 4, line 57 - page 6, line 9	1-15
A	KR 10-2005-0064905 A (LG ELECTRONICS INC.) 29 Jun. 2005 See abstract, figure 3, claims 1-3, and page 3, lines 1-15	1-15
A	KR 10-2001-0008959 A (SK TELECOM CO., LTD.) 05 Feb. 2001 See abstract, figures 1-2, claims 1-6, and page 3, line 11 - page 4, line 4	1-15

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

26 DECEMBER 2007 (26.12.2007)

Date of mailing of the international search report

27 DECEMBER 2007 (27.12.2007)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KIM, Kwang Sik

Telephone No. 82-42-481-8355



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/005155

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 06999991 B1	14.02.2006	None	
US 20020116472 A1	22.08.2002	W02003088064A1	23.10.2003
KR 1020030037448 A	14.05.2003	None	
KR 1020040045803 A	02.06.2004	None	
KR 1020050064905 A	29.06.2005	None	
KR 1020010008959 A	05.02.2001	None	



(11) **EP 1 853 044 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
14.01.2009 Bulletin 2009/03

(51) Int Cl.:
H04L 29/08 (2006.01)

(21) Application number: **06113378.1**

(22) Date of filing: **02.05.2006**

(54) **Push framework for delivery of dynamic mobile content**

Push-Architektur zur Zustellung von dynamischen mobilen Inhalten

Structure de Push pour distribution de contenus mobiles dynamiques

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI
SK TR**
Designated Extension States:
AL BA HR MK YU

(74) Representative: **Rickard, David John**
Ipulse
26 Mallinson Road
London
SW11 1BP (GB)

(43) Date of publication of application:
07.11.2007 Bulletin 2007/45

(56) References cited:
EP-A- 1 119 135 EP-A- 1 555 793

(73) Proprietor: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

• **HUANG Y-W ET AL: "A bandwidth-sensitive
update scheduling method for Internet push"
DISTRIBUTED COMPUTING SYSTEMS, 1998.
PROCEEDINGS. 18TH INTERNATIONAL
CONFERENCE ON AMSTERDAM,
NETHERLANDS 26-29 MAY 1998, LOS
ALAMITOS, CA, USA, IEEE COMPUT. SOC, US, 26
May 1998 (1998-05-26), pages 303-310,
XP010284011 ISBN: 0-8186-8292-2**

(72) Inventor: **Shenfield, Michael**
Richmond Hill,
Ontario
L4C 3S9 (CA)

EP 1 853 044 B1

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

[0001] The present method and system relate to dynamic content delivery in a mobile environment, and in particular to a generic dynamic content delivery architecture in which applications and content providers can be added without changing the architecture.

[0002] Users of mobile devices or mobile user equipment (UE) are increasingly becoming more sophisticated in terms of the functionality that they require from their mobile devices and the way that they access data from the mobile devices.

[0003] Dynamic content delivery allows users to have information or data pushed to them rather than having to go and seek out the data. Examples of data could include stock quotes, weather updates, traffic updates, dynamic wallpaper, ads, applications or other data desirable to a user.

[0004] Current technologies for mobile devices such as wireless application protocol (WAP) have the ability to push content; however, WAP requires websites to be rewritten to satisfy the wireless application protocol and provide users with a uniform site that does not change to accommodate a user's capabilities to view a site.

[0005] Other alternatives include SMS based push and broadcast or cell broadcast. In the broadcast case, delivery cannot be customized to the needs of a particular user or the capabilities of a particular device. These systems therefore have no intelligence associated with them. A better solution is required for mobile devices.

[0006] The present system and method preferably provide for a dynamic content delivery architecture and system that allows generic applications and content providers to be added to the system without the necessity to modify the architecture. Specifically, the present system and method allows for a mobile device to become a dynamic application platform in which applications can be added and content provided to the mobile device, where the architecture of the dynamic content delivery system does not limit the type of application that can be installed on the device nor the type of content that the device receives.

[0007] In one aspect of the present application, metadata is preferably provided and associated with the content to add intelligence to the content for various processing elements within the dynamic content delivery architecture. This architecture includes logical components that provide for content provision, service provision including push proxies, a wireless network, push client and client applications.

[0008] In a further aspect of the present application, metadata is preferably provided in a layered "enveloped" model for push content metadata. Content is wrapped with metadata that can be used for processing at each element within a push framework. The metadata for each successive element is layered, thereby allowing the processing element to extract only the metadata for that element. For example, a content package that includes metadata directed to a push proxy and a client application can include the content with a first level of metadata for the client application, and a second layer of metadata for the push proxy. Thereby, when the envelope reaches the push proxy, the metadata for the push proxy is extracted and applied to the content, and the modified content and metadata for the client application is passed to further processing element.

[0009] In another aspect of the present application, the metadata can be split into static metadata (also referred to herein as channel metadata) and dynamic metadata (also referred to herein as content metadata). Static metadata is established preferably at the time of registration of both the application and the content provider. However, the channel metadata can be established at a later time. The channel metadata specifies processing rules that are specific to the type of content that is being delivered and the application requirements for content type.

[0010] Dynamic metadata is conversely associated with the specific content being passed.

[0011] In another aspect of the present application, a plug-in registration model is preferably presented within the push framework. A generic push client and a push proxy are identified, each having various processing blocks or modules that allow these elements to process both content and metadata. These blocks can be directed to process either the content being passed, the metadata being passed or both the content and the metadata being passed.

[0012] Plug-in registration further preferably provides for the passing of service manifests and application manifests to allow the establishment of channel metadata between a content provider and an application. Specifically, service manifests can be used for registering a content provider with the push framework, and an application manifest can be used for registering an application with the push framework.

[0013] In another aspect of the present application, a method for pushing syndicated content is preferably provided which allows for the handling of data based on its priority and based on network factors including the cost for sending data, the type of network connected to or the users' preferences. An optional mixed push/pull model for syndicated content allows for either a push proxy to push content when network conditions become favorable or for a client to pull content when network conditions become favorable or when the user requires the content.

[0014] In order to accommodate various mobile devices, a further aspect of the present application preferably provides for content fragmentation for content, including non-linear content fragmentation. Non-linear content fragmentation includes augmenting the content with metadata allowing the data to be recomposed once it has been passed to the client.

[0015] These and other aspects will be identified in more detail with respect to the drawings.

[0016] The present application therefore preferably provides a push proxy for use in a generic dynamic content delivery

system comprising: a content provider registration service provider interface, said service provider interface adapted to register content providers with said push proxy server and to further receive channel metadata for the content providers; a channel metadata repository, said channel metadata repository adapted to store said channel metadata received from the content providers; a content metadata extractor and cache module, said content metadata extractor and cache module being adapted to extract metadata for said push proxy from a content and metadata envelope received from the content providers, said content metadata extractor and cache module further adapted to cache said metadata on said push proxy; a content fragmentation module, said content fragmentation module adapted to break a content and metadata envelope into segments; a deferred retrieval message store module, said deferred retrieval message store module adapted to store a content envelope or one or more segments from said content fragmentation module; a content expiry and replacement module, said content expiry and replacement module adapted to expire content stored in the deferred retrieval message store module or to replace content stored in the deferred retrieval message store module; a content dependencies module, said content dependencies module adapted to provide selection of push clients to advertise a service to; a push scheduler, said push scheduler adapted to schedule the pushing of a content envelope stored in the deferred retrieval message store module; and a subscription and rules module, said subscription and rules module adapted to maintain a subscription between an application and the content provider and maintain a list of rules for the subscription. The may be adapted to register only one content provider or to register multiple content providers. The push proxy may further comprise a content storage module for storing content and a service administration module for administering said push proxy.

[0017] The present application further provides a push clients for use in a dynamic content delivery architecture, the push client comprising: an application registration application provider interface adapted to register applications to said push client and further adapted to receive an application manifest for said applications, said application manifest containing channel metadata; a channel metadata repository adapted to store channel metadata received from said application; communication means, such communication means adapted to receive a content and metadata envelope from a push proxy; content metadata extractor and cache module, said content metadata extractor and cache module being adapted to extract metadata for said push client from said content and metadata envelope and further being adapted to cache said metadata on said push client; a deferred retrieval manager adapted to schedule retrieval of content from the push proxy not yet received by the push client; a content dependencies module adapted to reconstitute content previously broken into segments; a content expiry and replacement module, said content expiry and replacement module adapted to expire content stored at said push client or to replace content stored at the push client; an update notification block, said update notification block adapted to work with said applications to notify the applications that new content is waiting for them; a subscription management block, said subscription management block adapted to manage subscriptions between the application and a content provider; a pull broker adapted to pull content when required by the push client, said pull broker being driven by aid deferred retrieval manager, wherein said push client is adapted to register generic applications and receive generic content type from the content provider. The push client may be adapted to register with only one application or to register with multiple applications. The push client may further comprise a content storage module for storing content and a service administration module for administering said push client.

[0018] The present application preferably provides a method of pushing generic dynamic content via a push proxy of a generic dynamic content delivery system, the method comprising: obtaining a service manifest at the push proxy, the service manifest corresponding to a dynamic content push service provided by a service provider; registering a content provider with the generic dynamic content delivery system by registering the content provider with the push proxy having a content provider registration interface to receive channel metadata from the content provider; storing said channel metadata in a channel metadata repository associated with the push proxy; receiving a content and metadata envelope at the push proxy from the content provider; and processing the content and metadata envelope in accordance with the channel metadata. The method may comprise receiving said channel metadata from the content provider. The method may further comprise administering said push proxy.

[0019] The present application preferably provides a method of pushing generic dynamic content via a push client of a generic dynamic content delivery system, the method comprising: obtaining an application manifest at a push client, the application manifest corresponding to an application processing dynamic content pushed thereto; registering the application with the generic dynamic content delivery system by registering the application with the push client having an application registration interface, said application manifest containing channel metadata; storing said channel metadata in a channel metadata repository associated with the push client; receiving a content and metadata envelope at the push client via a push proxy; and processing the content and metadata envelope in accordance with the channel metadata. The method may further comprise receiving said channel metadata from said application. The method may further comprise notifying said application of new content waiting therefore and managing subscriptions between the application and the content provider. The method may further comprise any of administering said push proxy, performing background updates for applications not connected with said push client, storing content for said application at a specific storage vocation, notifying said application that data has been stored at the specific storage location, and sending said content and metadata envelope to said application.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The present application will be better understood with reference to the drawings, in which:

5 **Figure 1** is a block diagram of a basic architecture for a dynamic content delivery system;
Figure 2 is a block diagram showing alternative architectures of the dynamic content delivery system of **Figure 1**;
Figure 3 is the block diagram of **Figure 1** showing content and metadata flow;
Figure 4 is a block diagram showing a push proxy that can be used in association with the present system and method;
Figure 5 is a block diagram showing a push client that can be used in association with the present system and method;
10 **Figure 6** is a block diagram showing a multilayer envelope model of content and metadata;
Figure 7 is the block diagram of **Figure 6**, showing processing steps dynamic metadata for each envelope;
Figure 8 is the block diagram of **Figure 6**, additionally showing processing using static and dynamic metadata;
Figure 9 is a block diagram showing a registration process for an application to a single shared push client;
Figure 10 is a block diagram showing a registration process of an application to a push container managing a pool
15 of push clients;
Figure 11 is a block diagram showing an application registering to a content processor and socket listener;
Figure 12 is a block diagram showing a content provider registering with a single shared push proxy;
Figure 13 is a block diagram showing a content provider registering with a push container managing a pool of push
proxies;
20 **Figure 14** is a flow diagram showing registration messages between a content provider and client application;
Figure 15 is a block diagram showing interaction during registration between a push client and push proxy;
Figure 16 is a block diagram showing interaction during registration between a push proxy and a content provider;
Figure 17 is a flow diagram showing the flow of content and metadata between a content provider and processing
elements;
25 **Figure 18** is block diagram showing an exemplary transform application for content;
Figure 19 is a block diagram of a content syndication model;
Figure 20 is a block diagram of a linear fragmentation process;
Figure 21 is a block diagram of a non-linear fragmentation process; and
Figure 22 is a block diagram of an exemplary mobile device that could be used in association with the present
30 method and system.

DESCRIPTION OF PREFERRED EMBODIMENTS

35 [0021] Reference is now made to Figure 1. A generic push system for delivering dynamic content to a client application is illustrated. A system of Figure 1 is a simplified system and shows logical components that need to be in a dynamic content delivery architecture; however, one skilled in the art will appreciate that other components could exist or that various components could be grouped together.

40 [0022] Architecture 100 includes a content provider 110. Content provider 110 is arranged to provide dynamic content to users that are subscribed with content provider 110. Examples can include, for example, a website selling books. A user may register with content provider 110 to obtain a list of newly released books within specified genres. Other examples could include news sites which might provide headlines to users on a periodic basis, traffic sites which might provide up-to-date traffic information to users during certain periods of the day, stock market sites which could provide updated stock quotes or currency exchange rates to users, among others.

45 [0023] As will be described in more detail below, content provider 110 registers with a service provider 120 in order to allow clients of the service provider to receive content from content provider 110. Service provider 120 includes a push proxy 122 that acts as a proxy for a client or a client application and provides a destination for content provider 110 to send content.

50 [0024] Service provider 120 communicates over wireless network 130 with a push client 140 that is located on a mobile device. Push client 140 will be described in more detail below. Push client 140 receives the content that is being delivered from content provider 110 and can communicate the content with a client application 150, which ultimately consumes the content.

[0025] Within the present specification, reference to content provider 110, service provider 120, push proxy 122, wireless network 130, push client 140 or client application 150 is a reference back to the architecture of Figure 1.

55 [0026] Referring to Figure 2, it will be appreciated by those skilled in the art that the components of Figure 1 are merely logical components and are not necessarily separate physical components. Figure 1 illustrates a generic architecture in which one content provider 110, one push proxy 122, one push client 140 and one client application 150 exist. Alternatives are illustrated in Figure 2.

[0027] Specifically, a first alternative architecture 210 includes multiple content providers 110 communicating with a

push proxy 122. Push proxy 122, as in the architecture of Figure 1, communicates over wireless network 130 with a push client 140. Further, multiple client applications 150 exist in architecture 210. This is therefore an N-1-1-N system having multiple content providers 110 and multiple client applications 150.

[0028] Architecture 220 of Figure 2 includes one content provider 110 communicating with and registered to push proxy 122. Further, push proxy 122 communicates over wireless network 130 with multiple push clients 140. Each push client 140 communicates with a client application 150. Architecture 220 therefore groups the logical components of a client application 150 and a push client 140 and is an N(1-1)-1-1 system.

[0029] Architecture 230 of Figure 2 has multiple push proxies 122, each communicating with a content provider 110. Each push proxy and content provider combination 232 communicates over wireless network 130 with a generic push client 140, which in turn communicates with client application 150. This is an 1-1-N(1-1) system.

[0030] In architecture 240 of Figure 2, a content provider 110 and push proxy 122 grouping 232 communicates over wireless network 130 with a generic push client 140 and client application 150 combination. This is therefore an N(1-1)-N(1-1) system.

[0031] As will be appreciated by those skilled in the art, other alternatives are possible. The above shows various logical components, which can be in separate physical components or grouped together. For example, a push client can be imbedded in an application, common shared clients can be used by multiple applications or other alternatives.

[0032] Reference is now made to Figure 3. In order to add intelligence to a system, content is associated with a metadata. Metadata, in this case, is defined as data that can be used by a processing element to manipulate the content. As will be appreciated, a generic push system requires metadata to allow various content providers and applications to exist within the system. The metadata can be in various forms, including processing parameters or rules, or a processing handler, code or reference provided directly or a link to a processing handler, code or rules in another location,

[0033] As can be seen in Figure 3, content passes from content provider 110 to client application 150 and is illustrated by arrow 310. Metadata, which provides instructions to various components within the architecture 100 can also pass between components within architecture 100, usually along with the content. For example, arrow 320 illustrates metadata that originates at the content provider and is transparent to the delivery system until it reaches a client application 150.

[0034] Arrow 330 shows metadata created by content provider 110 that is intended for the push client 140, and thus only flows to generic push client 140.

[0035] Arrow 340 illustrates metadata generated by service provider 120 and intended for the push client 140, and thus is first associated with the content at the push proxy 122 and stripped from the content at generic push client 140. Examples of where this could occur include agreements between a user and a service provider regarding a billing plan and the level of service to be provided, where the service provider can use the metadata to limit the services available or provide enhanced services.

[0036] The flow of metadata and the role of metadata is described in more detail below.

[0037] Reference is now made to Figure 4. Figure 4 illustrates a detailed exemplary push proxy 410 which can be used in association with the present system and method. As will be appreciated by those skilled in the art, push proxy 410 could be the same as push proxy 122 from Figures 1 and 2.

[0038] Push proxy 410 of Figure 4 includes various elements that enable push proxy 410 to operate in a generic push environment. This facilitates flexibility since the push proxy is not limited to interaction with specific content providers or push clients, but instead can be adapted to a dynamic environment. The elements described below for push proxy 410 are preferable have within push proxy 410, but the elements are not exhaustive, and other elements are possible. Further, certain elements may be omitted from push proxy 410, with the remaining elements still able to perform generic push services.

[0039] Push proxy 410 includes content providers 412 registered to it. Content providers 412 register with a content provider registration service provider interface (SPI) 420. As is described in more detail below, it is desirable in this registration that the content provider 412 includes certain information for the channel being established, referred to herein as channel metadata. Content providers 412 can be the same as content providers 110 of Figure 1.

[0040] Push proxy 410 further includes a service administration block 430 to administer the push proxy service.

[0041] Push proxy 410 includes various modules to deal with both the content and the metadata associated with that content. A first module is the message broker and delivery queue 440, which is a subsystem that consumes messages from content provider 412 and manages the content delivery queue. As will be appreciated by those skilled in the art, not all content for all client applications can be delivered at once and a delivery queue needs to be established in order to deliver the content in due course. For example, a device may be out of coverage and content may need to be stored.

[0042] Push proxy 410 further includes a flow control management block 442. Flow control management block 442 allows for the control of content flow. For example, a mobile station with limited space may only be able to receive a certain amount of information. In this case, the mobile device, through a push client 140 as illustrated in Figure 1, may ask push proxy 410 to stop the flow of data to push client 140. The flow control management block 442 deals with this.

[0043] Alternatively, the mobile device can be off-line. Flow control management block 442 stops and starts the flow of data to push client 140 when content cannot be delivered as received by push proxy 410.

[0044] A further component of push proxy 410 is push agents 444. Push agents 444 are responsible for sending data to clients.

[0045] As will be appreciated by those skilled in the art, blocks 440, 442 and 444 deal with messaging only, and are not metadata related. In other words, the blocks handle the content of the messages, but not any metadata associated with the content.

[0046] A further component of push proxy 410 is the content metadata extractor and cache block 450. Content metadata extractor and cache block 450 operate on enveloped content metadata. Specifically, in the envelope model of metadata system, which is described in more detail below, each logical component within the system can have metadata associated with content processing. This metadata allows the logical component to perform actions on the content. Each logical component thus needs to be able to extract the metadata that is associated with it.

[0047] Content metadata extractor and cache block 450 is responsible for extracting metadata that is associated with push proxy 410 and for caching this metadata. The caching function allows optimization by eliminating the need to pass identical metadata in subsequent content envelopes from the same content provider. The extraction and caching of metadata are described below.

[0048] Deferred retrieval message store block 452 is used when it is not effective to deliver content, or parts of it, to a client application. The deferred retrieval message store block 452 can be used to store content that is not delivered to the client until it is effective to send the content, or until the content is pulled by the client. The deferred retrieval message store could also be used to cache auxiliary content that could be optionally send to or pulled by the client depending on client application navigation through already delivered content.

[0049] The purpose of deferred retrieval message store block 452 is better explained below with reference to Figure 19 and 21. By way of example, deferred retrieval message store block 452 may be used is the case where a user has requested location information, such as a restaurant close to the location of the user. The content provider or the service provider may have a model of providing information where advertisers can pay to add their information to search requests. Thus, the user that's requesting restaurant information for a location may also have information about stores, golf courses, gyms or other services close to their location attended to their request. A content provider bundles the restaurant information requested with the additional information and passes it to push proxy 410.

[0050] Push proxy 410 can, based on the metadata provided, create a content package to send to the client. The content package could include the information requested by the client, as well as a digest or summary of related information that the user may be interested in. The summary is sent to the user, but the deferred retrieval message store block 452 stores the actual data that was received from content provider 110. Thus, if in the future the user wishes to obtain more detailed information about information within the digest, this information is already stored at push proxy 410.

[0051] An alternative use for deferred retrieval message store block 452 is in the case where a user cannot accept the entire content at once. For example, if it is not feasible or economical to send all content to device, part of the content can be stored until a later time, when it can be pulled by the client or pushed when predefined rules are met. These rules can be specified by the network or service conditions by certain network or service conditions being satisfied. This is described in more detail with reference to Figure 19 below.

[0052] Push scheduler 454 schedules delivery slots for clients. As described above, in some situations it may not be efficient to push all of the content at once. Push scheduler 452 can determine that it will push some information immediately and the rest according to a predefined schedule. Also, push scheduler 454 may use nature of the content to determine when the content should be pushed. Specifically, metadata may indicate that some content is a high priority or has an expiry that is limited in time, and this content may be pushed immediately, whereas content that has been indicated to have a low priority or with no expiry may be pushed later when conditions for passing data are more favorable.

[0053] As will be appreciated by those skilled in the art, blocks 450, 452 and 454 deal with both the content of the message and the metadata that is associated with the message.

[0054] Subscription and rules block 460 tracks applications that are registered to receive a service and monitors rules on how to handle particular content being delivered. Content is typically delivered based on a subscription by the client or on behalf of the client. The user, for example if they want a particular service, can actively request subscriptions. Subscriptions can be made on behalf of a user, for example, if the user has signed an agreement with their service provider 120 to receive a benefit for a service. This could include the case where a user receives a preferred rate as long as the user agrees to receive a certain number of advertisements each day. In this case, the service provider 120 may make the subscription to the advertisement provider on behalf of the client.

[0055] When an application is deleted on a mobile device or when the application unregisters from a subscription, subscription and rules block 460 can unsubscribe that user.

[0056] Content dependencies block 462 is used by push proxy 410 to advertise services that a mobile device user can utilize. Thus, if a mobile device user does not have a screen or bandwidth or memory sufficient for the service, content dependencies block 462 could block the advertisement of that service to the user.

[0057] Content fragmentation block 464 is used to fragment content. This could be used, for example, if the mobile device is unable to receive all of the content at once. Content fragmentation block 464 is used to break the content into

various components. It can be used in association with deferred retrieval and message store 452 to store fragmented content that has not yet been delivered.

[0058] Content expiry and replacement block 466 is used for two purposes. First, this block can be used to monitor subscriptions. Each subscription has an expiry time and when this expiry time is met, the subscription can be ended.

[0059] Also, content expiry and replacement block 466 can be used to monitor information. Certain content will have time limits on the validity of the information. For example, a traffic application used to monitor rush hour traffic will be very time dependent. If, for some reason, push proxy 410 is unable to deliver the content immediately to a mobile device, this content is stored in content storage 480 for future delivery. However, if the content is not delivered within a certain specified time period, then it could expire and not be delivered at all.

[0060] Similarly, content replacement deals with a situation where the information is being updated. For example, a client application that is receiving stock quotes may only want the latest stock quote. Thus, if the push proxy 410 is unable to deliver the stock quote to push client 140 and a subsequent stock quote is received from a content provider 110, metadata within the subsequent stock quote can indicate that it should be used to replace the previous stock quote. Replacement of stored information rather than adding all information to a delivery queue frees space within content storage 480.

[0061] Channel metadata repository 470 is used to store channel metadata, which is described in more detail below.

[0062] The above describes an exemplary push proxy 410 that can be used with the method and systems herein. The blocks and elements of push proxy 410 allow push proxy 410 to be used in a generic dynamic content delivery system where the type of content and handling of the content at an application can vary and is not predetermined.

[0063] Reference is now made to Figure 5. Figure 5 illustrates a push client 510 that can be used in association with the system and methods herein. Push client 510 can be the same as push client 140 from Figures 1 and 2.

[0064] As will be appreciated by those skilled in the art, a push client 510 that is to be used in a generic system in which the content and processing of the content is not predetermined should include blocks or modules that can be used to accommodate both the content and the metadata associated with the content. The blocks defined with regard to Figure 5 are not meant to be exhaustive, and other blocks could also exist within a push client 510. Further, the blocks within push client 510 can, in some instances, be omitted without restricting the functionality of the other blocks within push client 510.

[0065] A push client 510 services applications, and one or more applications 512 can register with push client 510. The application registration uses an application provider interface 514 as the interface for registration and application provider interface 514 can further be used to extract channel metadata for the application, as described in more detail below.

[0066] Push client 510 includes client administration 520 used to administer the push client 510.

[0067] As with push server 410 of Figure 4, push client 510 includes various blocks that deal with messaging, various blocks that deal with metadata, and various blocks that deal with both messaging and metadata.

[0068] Message broker and application queues 540 handle messages from push proxy 410 for delivery to applications 512. An application queue is a queue of messages for applications 512.

[0069] Flow control management block 542 is used to notify push proxy 410 of Figure 4 to stop pushing content or to resume pushing content. This can be used, for example, when the push client 510 has a limited amount of memory that it can accept pushed content. In this case, before the push content is consumed push client 510 needs to stop the flow of content from push proxy 410. Once the content has been consumed, flow control management block 542 can be used to start the flow of data again.

[0070] Push agents 544 within push client 510 are used to receive information from push proxy 410 of Figure 4.

[0071] As will be appreciated by those skilled in the art, message brokers and application queues 540, flow control management block 542, and push agents 544 deal exclusively with messaging and not with metadata.

[0072] Content metadata extractor and cache block 550 is used to extract dynamic metadata destined for push client 510. As indicated above with reference to push proxy 410 of Figure 4, any of the processing elements in the dynamic content delivery architecture could have metadata destined for them and this metadata needs to be extracted. Thus metadata destined for push client 510 is extracted by content metadata extractor and cache block 550.

[0073] Further, the content metadata extractor and cache block 550 is preferably adapted to cache metadata. Metadata for push client 510 that does not change between a first content package and a second content package does not need to be passed, saving processing time at push client 510 by not requiring the extraction of this metadata, and further saving network resources by not requiring metadata for push client 510 to be passed over wireless network 130.

[0074] Deferred retrieval manager 552 is used for analyzing fragments of content that are received and putting the content together in the correct way. As described in more detail below, data can be either linear or non-linear. If the data is non-linear, then metadata is required in order to reconstitute it, and this is done by deferred retrieval manager 552. The deferred retrieval manager 552 also is adapted to analyse a digest of information available in the deferred retrieval store 452 of push proxy 510 and drives the content pull broker 554 (described below) to retrieve this information when required by user. This includes predictive retrieval when content navigation enters a certain branch of the content structure

graph or when bandwidth or cost conditions are satisfied

[0075] Content pull broker 554 is used in a push/pull model where the push client 510 is also able to pull content in certain situations. Such situations are described below in more detail with reference to Figure 19.

[0076] As will be appreciated by those skilled in the art, content metadata extractor and cache 550, deferred retrieval manager 552 and content pull broker 554 deal both with messaging content and with metadata.

[0077] Subscription management block 560 is the same as subscription and rules block 460 of Figure 4. Specifically, subscription management block 560 is used to manage subscriptions. If an application de-registers or is deleted from a mobile device then subscription management block 560 ends the subscription. The subscription management block 560 can also re-subscribe on behalf of a client application when subscription channel expires.

[0078] Update notification block 562 works with client applications and is used to notify the applications that new content is waiting for them. This can be done in one of three ways:

a. A first way that update notification block 562 can notify an application 512 is for push client 510 to send the content to application 512 directly.

b. A second way that update notification block 562 can notify applications 512 of new content is to store the content in content storage 580 and to optionally notify applications 512 that content is waiting. Notification in this case is optional. Specifically, if an application 512 knows that information destined for it is stored within a specific memory block, one option for the application discovering that it has new data is to periodically poll the memory location to see whether there has been something written to it. Alternatively update notification block 562 can send a message to application 512 indicating that it has new data and possibly the location that the data is stored.

c. A third way that update notification 562 can notify applications 512 of new content is to store the content internally and notify the application. The application can then call on the push client to retrieve the content.

[0079] Content dependency block 564 is the same as content dependency block 462 of Figure 4, and can determine whether to advertise the service to the mobile device.

[0080] Content expiry and replacement block 566 is the same as content replacement and expiry block 466 of Figure 4. The expiry of content and replacement of content can thus be handled at push client 510 in addition to the push server or push proxy.

[0081] Channel metadata repository 570 is used to store channel metadata for application 512.

[0082] Background update processing module 575 is used for performing updates when an application 512 is unavailable. The background update allows, for example, the replacement of data with newer data inside the application storage. Thereafter, when a user starts the application, the data displayed by the application is correct and updated.

[0083] Background update processing module 575 uses processing rules translate content into a format acceptable for an application. It can execute and process content in content store 580.

[0084] By way of example, a task list that is updated for a contractor overnight could have tasks pushed to it. The task application is not started during this time, and background update processing module 575 can be used to update the content for the task application. This could be done with code for handling an extensible mark-up language (XML) file, and could exist on the device in a file called "handler.exe". Background update processing block 575 on push client 510 can run handler.exe, passing the XML document has a parameter. The handler then constructs the task into the application's internal format.

[0085] Once the background update processing block 575 of push client 510 constructs the task into the application internal format, it then can read the task into the task list from content storage 580 and append the new task to the list. It then can store the modified back to content storage 580 for when the task application next connects to push client 510.

[0086] Figure 5 therefore illustrates a push client 510 that can be used in a generic dynamic content delivery system, where content and processing of the content is dynamic and not predetermined. The blocks described above with reference to the push client 510 of Figure 5 are used to accommodate the dynamic nature of the system.

[0087] As indicated above with reference to Figure 3, content is associated with metadata to provide intelligence for the processing of the content. In accordance with the present method and system, metadata can be divided into two types of metadata. Specifically, static (channel) metadata and dynamic (content) metadata.

[0088] Due to the unlimited possibilities of types of content providers and applications, metadata is critical in order to build generic systems. The only way to handle the specific type of content is through metadata.

[0089] Static metadata is metadata that provides rules on how to process specific types of content. Static metadata can be broken into various levels of abstraction and include for example structural information about the content itself. For example, a Real-time Simple Syndication (RSS) document could be delivered with an RSS 2.0.XSD structure, and all content from that content provider will be delivered with this structure.

[0090] A further level of abstraction for static metadata includes the provision of processing rules for content subtype. This could be application specific. Thus, for example, a financial news application indicates that data should be extracted from a financial news RSS stream, stored in a predefined location, and that the application should be notified about the

arrival of the information. The application always requires content destined for it to be handled in this way.

[0091] The static metadata (also referred to herein as channel metadata) stays the same throughout the subscription between the application and the content provider, and thus the static metadata can be established once for each element within the architecture and for each content delivery channel. In one embodiment this is done at the time of registration of the application or the content provider.

[0092] Dynamic metadata is metadata that is associated with a particular piece of content. For example, expiry information associated with a particular piece of data or replacement rules and information associated with a particular piece of data (i.e. document K replaces document L).

[0093] As indicated above with reference to **Figures 4 and 5**, each processing entity can receive both static and dynamic metadata that is directed at that processing entity. Thus push proxy **410** uses the content metadata extractor and cache **450** to extract the dynamic metadata, and content expiry and replacement block **466** is used to replace undelivered content with newer content received at push proxy **410**.

[0094] Reference is now made to **Figure 6**. **Figure 6** illustrates a multilayer envelope model for content metadata.

[0095] A push proxy **410** receives a push envelope **610** that includes content processing metadata for the proxy server **612** and a push client envelope **614**. The push proxy **410** extracts content processing metadata **612** and uses this metadata to process push client envelope **614**. Metadata **612** dictates to push proxy what to do with the push client envelope **614**.

[0096] Push client envelope **614** is passed to push client **510** where it is broken into a content envelope **620** and a content processing metadata **622**. Content processing metadata **622** is used by push client **510** to process the content envelope **620**. For example, this can be used to instruct push client **510** to perform replacement of previously delivered content envelope **620** with the latest envelope if client application **150** is only interested in the latest version of the content.

[0097] Content envelope **620** is passed to client application **150**. Content envelope **620** includes content processing metadata **630** for the application and the content payload **632** that is to be consumed by client application **150**.

[0098] As will be appreciated by those skilled in the art, the nesting of envelopes in accordance with **Figure 6** provides for a rich dynamic environment in which processing can occur at any processing element of the architecture and which the content provider **110** can specify how specific content is to be dealt with. In one embodiment, metadata directed to a particular logical element is opaque to other processing elements.

[0099] Alternatively, the service provider **120** can also add metadata at push proxy **410** for processing at push client **510** or client application **150**.

[0100] Referring to **Figure 7**, this figure shows the envelope model of **Figure 6** and the steps that each processing element takes with an envelope. As illustrated in **Figure 7**, push proxy **410** first extracts the metadata from push envelope **610**. This is done in step **710**.

[0101] In step **712**, push proxy **410** uses the metadata to process the push client envelope **614**. In step **714**, push proxy **410** delivers the push client envelope **614** to push client **510**.

[0102] Similarly, push client **510**, in step **720** extracts the content processing metadata **622** from push client envelope **614**. In step **722**, push client **510** uses the content processing metadata **622** on content envelope **620**. In step **724**, the push client **510** delivers content envelope **620** to client application **150**.

[0103] In step **730**, client application **150** extracts the content processing metadata **630** and in step **732** uses the content processing metadata **630** on content payload **632**.

[0104] Referring to **Figure 8**, this figure shows the method as illustrated in **Figure 7** with the additional step of the use of static or channel metadata. Specifically, after the metadata has been extracted in step **710** from push envelope **610**, the push proxy **410** next uses the static channel metadata to process the push client envelope in step **810**. In step **712**, push proxy **410** next processes the content processing dynamic metadata **612**. Push proxy **410** next delivers the push client envelope **614** in step **714**.

[0105] Similarly, push client **510** extracts the content processing metadata **622** in step **720**. Push client **510** then uses the channel metadata in step **820** on the content within content envelope **620**. Push client **510** then, in step **722**, uses the dynamic content metadata in content processing metadata **622** prior to delivering content envelope **620** to client application **150** in step **724**.

[0106] Client application **150** first extracts, in step **730**, content processing metadata **630**. It then uses the channel metadata in step **830** on content payload **632**. Client application **150** then uses, in step **732**, content processing metadata **630** on content payload **632**.

[0107] As will be appreciated by those skilled in the art, the above model therefore allows for both static metadata to be applied for the channel along with dynamic metadata that is associated with the particular content being sent.

[0108] Reference is now made to **Figure 9**. As will be appreciated from **Figure 5**, push client **510** can serve multiple target applications **512** on a mobile device. An efficient runtime registration mechanism is required where applications can register with the dynamic content delivery framework without interrupting service for other applications.

[0109] Referring to **Figure 9**, push client **510** includes three applications, specifically applications **910**, **912** and **914** that are already registered with the push client. As will be appreciated, the plug in model is important because new

devices can allow unlimited application types to be installed on the device. Further, applications can be installed dynamically, leading to a mobile device becoming an application platform. Because the device can be an application platform, it must be capable of dynamically incorporating new applications.

5 [0110] As seen in Figure 9, application 916 wants to register with push client 510. Application 916 includes an application manifest 918 that, in a preferred embodiment, provides the channel metadata for the application. Specifically, application manifest 918 provides information to push client 510, and ultimately push proxy 410 and content provider 110 from Figure 1 with the static metadata for the application. This can include, but is not limited to, what type of content the application expects, how the content will be delivered, whether the application needs notification, or other channel information that would be evident to those skilled in the art having regard to the present system and method.

10 [0111] Application 916 therefore registers with push client 510, providing application manifest 918 to establish a channel to a content provider for servicing application 916.

[0112] Referring to Figure 10, an alternate model could be the model described with regard to architecture 220 of Figure 2. Specifically, in the model of Figure 10, a client application 150 is paired with a push client 140. Each of the client application 150/push client 140 pairs are coordinated with a push container 1010.

15 [0113] When application 1020 wishes to register with push container 1010, a client 140 is created, or if it already exists is used, by push container 1010. Further, in registration, the application 1020 provides an application manifest 1030 to push container 1010, thereby providing channel metadata (static metadata) for application 1020.

[0114] An alternative illustration of Figure 10 is shown in Figure 11. Specifically, a push container 1110 manages/maintains a pool of push clients. When an application registers with the container it obtains a dedicated push client 510, which in the simple case could be represented by a pair of a socket listener 1130 and content handler. The push client is returned to the pool when the application unregisters from the container (and content delivery service) or is deleted from the device.

[0115] Push container 1110 includes sockets 1120 for communication. Further, push container 1110 includes socket listeners 1130 and content processors 1140 assigned to a particular socket.

25 [0116] As seen in Figure 11, various content processor and socket listener pairs are used by previously registered applications 150.

[0117] When a new application 1150 wants to register with push container 1110, a new content processor and socket listener 1120 and 1130 are assigned to service application 1050.

30 [0118] The above therefore provides for a generic push framework in which a client application 150 that is new can be implemented and registered with a push client 510 or push container 1010 or 1110, thereby allowing the device to become an application platform capable of dynamically incorporating new applications. The passing of an application manifest 1030 or 918 from Figures 9 and 10 above allows for the establishment of channel metadata, thereby allowing the content to be processed according to the application's requirements.

35 [0119] Referring to Figure 12, content providers 110 similarly need to register with a push proxy 410. As seen in Figure 12, push proxy 410 includes three content providers, namely, 1210, 1212 and 1214, already registered with push proxy 410. Content provider 1216 desires to register with push proxy 410.

[0120] Similarly to the application manifest 918 illustrated in Figure 9 provided by an application 916 when registering with push client 510, content provider 1216 includes a service manifest 1218 that is passed to push proxy 410 when content provider 1216 registers. Service manifest 1218 includes information concerning the type of information that the content provider will provide, how often it provides this information, the format of the information, and any other information that is useful for the service or for advertisement of the service. Other information is possible.

[0121] Push proxy 410 thus uses service manifest 1218 to establish channel (static) metadata for content provider 1216.

45 [0122] Referring to Figure 13, an alternative embodiment, represented by architecture 230 of Figure 2, is to have a push container with a number of push proxy 122 and content provider 110 pairings. As with Figure 12, various applications could already be registered with push container 1310, and in the example of Figure 12, applications 1312, 1314 and 1316 are already registered with push proxies 1313, 1315 and 1317 respectively.

[0123] A new application 1320 wants to register with push container 1310. Thus, push container 1310 creates a new proxy (not shown) or uses an existing proxy (not shown) with which it associates content provider 1320. Further, content provider 1320 provides service manifest 1322 to describe the content that content provider 1320 will be providing, thereby allowing the establishment of channel metadata.

50 [0124] As will be appreciated by those skilled in the art, the embodiments of Figures 9 and 10 show two options for push clients, either with shared applications or with dedicated push clients per application. One skilled in the art will realize that other embodiments are possible. Similarly, with respect to Figures 12 and 13, a push proxy with multiple content providers registered to it is shown or a dedicated push proxy for each content provider, and embodied in a push container is shown.

55 [0125] With reference to Figure 14, messaging between a content provider 110 and a client application 150 is shown. Content provider 110 provides a registration message to push proxy 410. This message can include the service manifest which can be used to provide channel metadata to push proxy 410. This is done in step 1410.

[0126] Content provider 110 may also or alternatively provide channel metadata in a subsequent message, as illustrated by step 1412.

[0127] Push proxy 410 then adds a service to a list of available services (the service catalogue) in step 1414.

5 [0128] An optional step in the example of Figure 14 is for push proxy 410 to notify push client 510 of the new service available in step 1416 and this notification may be propagated to a client application 110 in step 1418.

[0129] As will be appreciated by those skilled in the art, steps 1416 and 1418 are optional, and other alternatives include client application 150 pulling the service catalogue periodically from push proxy 410 to view new services.

10 [0130] When a user or service provider for client application 150 decides that client application 150 should subscribe to a service, it sends a subscription message in step 1420. The subscription message is further passed to push proxy 410 in step 1422.

[0131] Once push proxy 410 receives the subscription message in step 1422, two options are available. A first option is to send a message 1424 to content provider 110 for a subscription and then receive a message envelope that includes metadata back in step 1426. The metadata could be device or device type specific.

15 [0132] Alternatively, push proxy 410 may receive the subscription message in step 1422 and immediately, based on information already provided by content provider 110 and stored on push proxy 410 reply in step 1430 to push client 510. This reply is propagated to the client application 150 in step 1532. As will be appreciated, the reply can include channel metadata specific for content provider 110.

20 [0133] The difference in models can be dependent on who is customizing the data for the application. As will be appreciated, content provider 110 provides the best customization of content compared with other processing elements. However, service provider 120, through push proxy 410, can also provide for customization of content.

[0134] Further, as will be appreciated, the structure of the content could be dependent on the data that the application requires. For example, in a financial application, the application may want both stock quotes and currency rates. The following XML may be used:

```
25 <FIN>
    <quotes>
        <quote ticker = ABC>
            18.54
        </quote>
30    <quote ticker = XYZ>
        123.45
    </quote>
    </quotes>
    <rates>
        <rate id = "US-CAN">
35    1.15
        </rate>
        <rate id = "US-EURO">
            0.85
        </rate>
40    </rates>
    </FIN>
```

[0135] If the user only wanted quotes and no currency exchange, the structure could change to:

```
45 <FIN>
    <quote ticker = ABC>
        18.54
    </quote>
    <quote ticker = XYZ>
50    123.45
    </quote>
    </FIN>
```

[0136] The metadata can provide information to the application on the structure that of the data being passed.

55 [0137] Thus, two models exist. Static metadata can be provided to push proxy 410 and to push client 510 either during registration or afterwards. Alternatively, the metadata for push proxy 410 and push client 510 can be pre-provisioned, i.e. information is stored at a push client or a push proxy until an application registers with a client.

[0138] Reference is now made to Figure 15. Figure 15 shows logical steps that occur upon registration of an application with a push client 510.

[0139] Once an application registers with push client 510, a first step 1510 is to match the registered application with the content type required by the application. This is known from the application manifest 918 as illustrated in Figure 9.

[0140] A second step 1520 is to set up the environment for the application. These include but are not limited to storage and delivery options for the application. For example, an application may limit transmissions to a predetermined amount of data. The push client 510 in a flow control event, or if the application or client is out of touch, may require the caching of the data for the application and optionally to notify the application that data is waiting.

[0141] A third step 1530, is to notify push proxy 410 of the application settings. This includes for example available storage for the application or push client 510. As will be appreciated, push proxy 410 should not push more data than push client 510 can store. Thus, the application settings could include an upper limit of the data that is passed. Referring to Figures 4 and 5, this could invoke content fragmentation block 464 to fragment the content if it is greater than the application can process. Also, if the data is non-linear, content dependencies block 462 may be required to create metadata for content dependencies block 564 of Figure 5 in order to allow content dependencies block 564 to reconstitute the data.

[0142] Referring again to Figure 15, step 1530 can also indicate preference on data delivery. For example, the application may prefer certain types of data over others and these types of data may be given priority. Thus step 1530 can be used to establish a delivery schedule where data of type "A" is delivered immediately while data of type "B" can be delivered at a deferred time.

[0143] Reference is now made to Figure 16. When a content provider 110 registers with a push proxy 410, various steps are performed. A first step 1610 includes analyzing required client settings for content storage and delivery. This can be used, for example, for service advertisement in order to identify push clients 510 on devices capable of consuming content from content provider 110.

[0144] A second step 1620 allows push proxy 410 to set up the environment, including proxy storage, delivery options, transformation options, among others.

[0145] In step 1630, push proxy 410 can check whether the application is already registered to obtain content from a content provider 110. If this is the case, the application is ready to receive content and a notification from push proxy 410 to content provider 110 that the delivery channel is established and the application is ready for content can be sent.

[0146] Step 1630 can occur, for example, if an application is pre-installed on a device prior to content provider 110 coming on-line. Thus, the application is waiting for content provider 110 to become available or the application is of generic type (e.g. a browser or RSS Viewer) and is capable of consuming information from multiple content providers. In an alternative setting, if content provider 110 is already available before the application is installed, the notification step 1530 in Figure 15 can be used to initiate the content starting to flow from content provider 110 to a client application 150.

[0147] As will be appreciated with reference to Figure 16, client settings can include certain information such as the available storage size used for content partitioning, the queue size used for flow control, delivery scheduling including a push interval, whether the client is retrieving information from the proxy, creating a pseudo-push mode, customization options such as the screen size of a mobile device, among others.

[0148] As will be further appreciated, service catalogues may differ for different clients. For example, certain clients may be able to utilize more data, have a different screen size or other conditions which make the client more suitable for a content provider 110 than a device that cannot handle this amount of information, has a smaller screen size, etc. Thus, push proxy 410 can create a service catalogue for specific client applications based on knowledge of those client applications, and only those devices with that client application 150 installed can receive information concerning the content provider.

[0149] As will be further appreciated, in some cases the application may be installed based on a service provider and content provider without the user intervention. For example, if content provider 110 registers with push proxy 410, a user of a mobile device may have a contract obligation to accept a certain application. Thus push proxy 410 could notify push client 510 that it is ready to install an application and push the application to push client 510. This could, for example, include a user that has agreed to receive a certain number of ads each month in order to get a preferred rate on their mobile plan. The content provider 110 could be an ad provider and push proxy 410 may therefore push an advertisement displaying application to push client 510, which might be serviced by an application installer registered with push client 410, thereby having the content provider 110 and the service provider 120 entirely driving the process.

[0150] The above therefore provides for a plug-in registration model in a push framework where each application or content provider registers and provides an application manifest or service manifest respectively. The application manifest or service manifest is used to establish channel metadata at the push proxy 410 and push client 510 either during registration or subsequently. Thereafter, when an application 150 registers and a content provider 110 registers, content can start flowing between the application 150 and the content provider 110.

[0151] With reference to Figures 4 and 5, the channel metadata is stored in a channel metadata repository 470 and 570. It is, however, also advantageous to store dynamic metadata on the various processing elements within architecture 100 if the dynamic metadata is repeated. As will be appreciated, this will save processing on the push proxy 410 since

current metadata extractor 450 does not need to extract the same metadata over and over. Further, processing by various modules such as content expiry and replacement module 466 or 566 do not need to be updated for each piece of content that is passed. Since push proxy 410 could be working with a large number of push clients 510, this processing saving for each content message could be significant. Further, bandwidth could be saved by not having to pass the metadata over a fixed line between content provider 110 and push proxy 410 or over the air between push proxy 410 and push client 510.

[0152] Reference is now made to Figure 17. Figure 17 illustrates an example of run time flow where your last metadata version is stored by the processing element.

[0153] As seen in Figure 17, content provider 110 provides a content envelope which includes content $[C_1 + M(p, c, a)_1]$. This means that a first content payload is being sent along with metadata that includes proxy metadata, client metadata and application metadata. This is sent in step 1710.

[0154] At step 1712, push proxy 410 uses the proxy metadata as illustrated by the phrase "use $M(p)_1$ ". Further, in step 1714 the content plus the metadata that includes the client metadata and the application metadata is passed to push client 510.

[0155] In step 1716, push client 510 uses the client metadata and further in step 1718, passes the content payload to client application 150. Client application 150 uses, in step 1720 the application metadata and further consumes the content payload.

[0156] As seen in step 1722, a second content payload, designated by C_2 , has the same metadata as the first content payload. Because each processing element, namely, push proxy 410, push client 510 and client application 150, cached the metadata for content provider 110, the metadata does not need to be passed again but instead already resides on the processing element.

[0157] Thereafter, in step 1724 the push proxy 410 uses metadata that was previously cached for the push proxy 410. Similarly, in steps 1726 and 1728 the push client 510 uses the client metadata and the client application 150 uses the application metadata respectively. Content is passed, without metadata, in steps 1725 and 1727.

[0158] As illustrated in step 1740, content may have new metadata for the push client 510 and client application 150, but may keep the old metadata for the push proxy 410. In this case, the metadata that is passed in step 1740 includes only client metadata and application metadata. In step 1742, the push proxy 410 uses the cached proxy metadata and passes the content payload along with the new client metadata and application metadata in step 1744.

[0159] In step 1746, the push client 510 uses the new client metadata that was passed to it and further passes the content payload and application metadata in step 1748.

[0160] In step 1750, the client application uses the new application metadata and further consumes the content payload.

[0161] As will be appreciated by one skilled in the art, various configurations could exist concerning which metadata has changed and which metadata stays the same, and only the metadata that has changed is passed to the processing element that requires it. As will be appreciated by those skilled in the art, the processing element, if it does not receive new metadata, goes back to the cached metadata that it has stored and uses this on the content payload.

[0162] In a further alternative embodiment, incremental changes can also be made to metadata. For example, in step 1760 a new content payload along with a delta metadata version can be passed to service proxy 410. The delta of the proxy metadata can include a difference between the proxy metadata previously passed and the current metadata that the content should be processed with. The push proxy 410 composes the metadata by adding the previous metadata with the delta and then using this to process the content payload in step 1762. Thereafter, since there has been no change, in step 1764 the content payload is sent by itself and in step 1766 the push client 510 uses the previously cached client metadata.

[0163] Push client then passes the content payload in step 1768 to client application 150, which uses the previously cached location metadata on the content payload in step 1770 and then it consumes the content payload.

[0164] An example of where incremental data may be used is a situation in which a content provider tells the proxy that of the existent fields within the content payload, 30 should be extracted to send to client application 150. In a subsequent transaction, two additional fields that are important for that piece of content payload may be deemed necessary to be passed to the client application 150 by content provider 110. The content provider could therefore, using an incremental change, tell push proxy to extract the two additional fields and add them to the 30 fields that were previously extracted. By only having to pass the delta, i.e. the two additional fields, the processing time for extracting the metadata at push proxy 410 is reduced, thereby optimizing the process.

[0165] As will be further appreciated, metadata can come in various forms. It could be compiled such as native code or interpreted code such as Java or C#. The metadata can also be a data/properties file that indicates to use certain properties. In another alternative embodiment, it can be binary content, for example a transformation such as a XSLT transformation on an XML document.

[0166] The above can be used for various applications to provide intelligence for content being transferred to a specific client application. It can also provide for rich content providers that can provide content for various applications merely based on the metadata that they provide with their data. This can be illustrated by way of example in Figure 18.

[0167] A content provider 110 could, for example, be a on-line bookseller. An application can register with the on-line bookseller to indicate to the on-line bookseller that it wants to be informed of new releases of a specific genre. This could occur on a daily or weekly or monthly basis.

[0168] Content provider 110, for example, on a weekly basis will send a content envelope 1810 having a book list 1812, to push proxy 410. It can also send a transform metadata 1814, which can be, for example, a URL link for transforming the specific content based on the application receiving it.

[0169] In one embodiment, the book list 1812 could include numerous books, descriptions of each book including the author and a synopsis of the book. The file may, for example, be 100 KB in size.

[0170] Push proxy 410 can receive this large file and may realize, based on the client application being serviced, that a transformation to the large content file needs to be done in order to better accommodate the client which may only be able to receive, for example, 10 kilobytes of information. The transformation that is passed as a proxy metadata can therefore be applied to the book list to reduce the book list to a 10 KB modified document 1820. This can, for example, be done by removing the synopsis, ranking the books and only including the top 50 or other transformations as would be evident to those skilled in the art.

[0171] Once the transformation is complete, the modified document 1820 is then sent to the push client 510.

[0172] Further, the deferred retrieval message store 452, as seen in Figure 4, can be used to store the extra content that was stripped out in the transformation process.

[0173] The advantage of the above is that the bookseller can have one site and send one list to all of its clients. Since various clients will not be mobile wireless clients, the 100 KB file may be appropriate for these clients. By also providing the transformation metadata, the bookseller can have one list that it sends to everyone. As will be appreciated by those skilled in the art, most current web technologies require a separate website for a mobile client, and this is overcome by the above solution.

[0174] The above also lends itself to a syndication model and reference is now made to Figure 19.

[0175] As will be appreciated by those skilled in the art, a mobile device may not wish to receive large amounts of data when network conditions are not optimal for the receiving of large amounts of data. Further, network operators may wish to avoid sending large amounts of data during peak periods of bandwidth usage in order to spread network traffic more evenly over time. This can be accomplished using a push/pull model as illustrated in Figure 19.

[0176] As described with reference to Figure 4 above, content may be provided that includes more information than the user may currently needs. For example, if the user requests location information for restaurants within his area, a service provider may wish to add advertising such as other services available in the area. However, the service provider may not wish to push this additional content immediately to the user, but instead provide a primer such as a headline or a table of contents showing the additional content.

[0177] In other situations, the content may be too large to send to the user, and the user may receive only the first part of the content and the remainder of the content is stored in a deferred retrieval message store 452.

[0178] Thereafter, the stored content can be passed to push client 510 either by push proxy 410 or when asked for my push client 510.

[0179] Push client 510 includes a network status monitor 1910 which can monitor the status of the network. Push client 510 may wish to only receive extra data in certain conditions. For example, on a hybrid mobile device that has a WiFi and a cellular option, it is cheaper to provide data on the WiFi connection, and thus network status monitor 1910 could wait until the push client 510 is connected to a WiFi network prior to getting the deferred content. Alternatively, network status monitor could check whether the client is roaming in a foreign network or connected to the home network in order to minimize roaming charges. Network status monitor may also check to see whether a dedicated data channel is established for the device. One skilled in the art will realize that network status monitor 1910 could also check for various other preconditions in the network before requesting deferred data to be passed to push client 510.

[0180] A wireless network 130 could also provide information to either or both of push client 510 and push proxy 410 concerning the costs of delivery of data. As will be appreciated by those skilled in the art, various peak periods occur for the delivery of content. In the case of traffic information, the peak periods may be at the beginning and end of the workday when people are coming to and going from work. For stock quotes the peak period may be during the time that the market is open. Other peak periods will exist. In order to average the data traffic, it may be desirable for the network to charge different rates based on the current data usage in the network. Thus during peak periods a higher rate may be charged than a non-peak period such as the middle of the night. Wireless network 130 therefore provides delivery cost notifications to a deferred retrieval manager 552 on a push client 510 and to push scheduler 454 on push proxy 410.

[0181] In one embodiment, data from content provider 110 and passed to push proxy 410 can be ranked based on its importance to the client. Certain information can be designated through metadata to be delivered immediately. Other information can be designated to be delivered when the network cost is less than a first value (for example 10¢ per megabyte) and other data may be designated to be delivered when the network costs drop below a second value (for example, 5¢ per megabyte). Thus push scheduler 454 considers the data that is stored in deferred retrieval message store 452 and instructs push agent 444 to pass deferred data to push agent 544 on push client 510.

[0182] Alternatively, deferred retrieval manager 552 could also monitor network conditions as sent from wireless network 130 and if the data rate is below a certain rate can ask content pull broker 554 to pull content from deferred retrieval message store 452.

[0183] Alternatively, deferred retrieval manager 552 could see that the network status is favorable for pulling larger amounts of data, such as if the mobile device has connected with a WiFi network, and ask content pull broker 554 to pull the data from deferred retrieval message store 452.

[0184] As will be further appreciated, a user can always request to have the content pulled. Thus user request 1940 could also be used to trigger content pull broker 554 to pull the data from deferred retrieval message store 452.

[0185] The rules stored in push scheduler 454 and deferred retrieval manager 552 could be static metadata based on a classification of content. The rules could also be based on dynamic metadata for the particular data that has been passed. In this case the content provider 110 has classified the data.

[0186] Reference is now made to Figure 20. As will be appreciated by those skilled in the art, data can be one of two forms, linear or non-linear. Linear data could, for example, be arrays or strings or content that flows in a linear fashion. Non-linear data, conversely, is data that does not linearly relate to each other and can include complex dependencies with content maps or links.

[0187] For linear content, fragmentation merely involves the breaking of the data into various components based on linear progression. The data is partitioned into segments and the segments are delivered to the push client 410. As indicated in Figure 20, fragmentation processor 2010 interacts with content 2012 and decides that the content can be parsed with linear progression. The fragmentation processor 2010 next partitions the data into segments 2014, 2016 and 2018 in the example of Figure 20, and, as illustrated in Figure 20, passes the first segment 2014 while deferring the passing of the second and third segments 2016 and 2018 respectively.

[0188] The cursor management module 2030 keeps track of which segment has been delivered and delivers the next segment in order.

[0189] Referring to Figure 21, non-linear content needs to be partitioned in a more intelligent way. Further, at the other end, in order to reconstitute the segments, metadata is required.

[0190] A fragmentation processor 2110 analyses the content based on a metadata based analysis. These could include keeping certain segments or data elements together if logically required. Fragmentation processor 2110 analyses content 2112 and partitions the content into segments based on logical rules. Each segment includes the content plus metadata including for example, dependencies, maps, and navigation rules for each segment.

[0191] Once partitioned, a first segment 2114 is sent to push client 510 and the passing of the remainder of the segments 2116 and 2118 is deferred as illustrated in Figure 21. Segment navigation block 2130 deals with which segment to send next. As will be appreciated by those skilled in the art, first segment 2114 includes a data portion and a metadata portion. The metadata portion of segment 2114 is a layer of metadata that is added by the fragmentation processor 2110 to indicate to content dependencies module 564 how to reconstitute the content. Data portion of first segment 2114 can include both content and metadata associated with the channel or with the content.

[0192] Segment navigation block 2130 is adapted to process how a user travels through the data. For example, if the data is in a tree format and the user goes down a first branch of the tree, segment navigation block 2130 may pass to push client 410 other branches in the tree that can be reached from the element that the user has navigated to.

[0193] For example, a tree could include an employee database that has employee names along with a structure for the corporation. Based on Figure 21, if the user navigates into a specific department of the organization, the segmentation navigation block 2130 might forward the group fragments for groups within that department. If the user then navigates into a specific group within the department, the segmentation navigation block 2130 might then pass information fragments about the employees within that group.

[0194] The above therefore requires that the data be partitioned into logical components. Identifiers are assigned to all types and content, and structural information is created passing the information with the primer.

[0195] The above therefore provides an architecture for dynamic content delivery that can be used with generic systems where applications and content can be added without changing the structure of the system. The content can be tailored to fit the application receiving it, and be fragmented according to the above.

[0196] As will be appreciated, the push client and client applications can reside on any mobile device. One exemplary mobile device is described below with reference to **Figure 22**. This is not meant to be limiting, but is provided for illustrative purposes.

[0197] **Figure 22** is a block diagram illustrating a mobile station apt to be used with preferred embodiments of the apparatus and method of the present application. Mobile station **2200** is preferably a two-way wireless communication device having at least voice and data communication capabilities. Mobile station **2200** preferably has the capability to communicate with other computer systems on the Internet. Depending on the exact functionality provided, the wireless device may be referred to as a data messaging device, a two-way pager, a wireless e-mail device, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device, as examples.

[0198] Where mobile station **2200** is enabled for two-way communication, it will incorporate a communication subsys-

tem **2211**, including both a receiver **2212** and a transmitter **2214**, as well as associated components such as one or more, preferably embedded or internal, antenna elements **2216** and **2218**, local oscillators (LOs) **2213**, and a processing module such as a digital signal processor (DSP) **2220**. As will be apparent to those skilled in the field of communications, the particular design of the communication subsystem **2211** will be dependent upon the communication network in which the device is intended to operate.

[0199] Network access requirements will also vary depending upon the type of network **2219**. In some CDMA networks network access is associated with a subscriber or user of mobile station **2200**. A CDMA mobile station may require a removable user identity module (RUIM) or a subscriber identity module (SIM) card in order to operate on a CDMA network. The SIM/RUIM interface **2244** is normally similar to a card-slot into which a SIM/RUIM card can be inserted and ejected like a diskette or PCMCIA card. The SIM/RUIM card can have approximately 64K of memory and hold many key configuration **2251**, and other information **2253** such as identification, and subscriber related information.

[0200] When required network registration or activation procedures have been completed, mobile station **2200** may send and receive communication signals over the network **2219**. As illustrated in Figure 22, network **2219** can consist of multiple base stations communicating with the mobile device. For example, in a hybrid CDMA 1x EVDO system, a CDMA base station and an EVDO base station communicate with the mobile station and the mobile station is connected to both simultaneously. The EVDO and CDMA 1x base stations use different paging slots to communicate with the mobile device.

[0201] Signals received by antenna **2216** through communication network **2219** are input to receiver **2212**, which may perform such common receiver functions as signal amplification, frequency down conversion, filtering, channel selection and the like, and in the example system shown in Figure 22, analog to digital (A/D) conversion. A/D conversion of a received signal allows more complex communication functions such as demodulation and decoding to be performed in the DSP **2220**. In a similar manner, signals to be transmitted are processed, including modulation and encoding for example, by DSP **2220** and input to transmitter **2214** for digital to analog conversion, frequency up conversion, filtering, amplification and transmission over the communication network **2219** via antenna **2218**. DSP **2220** not only processes communication signals, but also provides for receiver and transmitter control. For example, the gains applied to communication signals in receiver **2212** and transmitter **2214** may be adaptively controlled through automatic gain control algorithms implemented in DSP **2220**.

[0202] Mobile station **2200** preferably includes a microprocessor **2238** which controls the overall operation of the device. Communication functions, including at least data and voice communications, are performed through communication subsystem **2211**. Microprocessor **2238** also interacts with further device subsystems such as the display **2222**, flash memory **2224**, random access memory (RAM) **2226**, auxiliary input/output (I/O) subsystems **2228**, serial port **2230**, two or more keyboards or keypads **2232**, speaker **2234**, microphone **2236**, other communication subsystem **2240** such as a short-range communications subsystem and any other device subsystems generally designated as **2242**. Serial port **2230** could include a USB port or other port known to those in the art.

[0203] Some of the subsystems shown in Figure 22 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard **2232** and display **2222**, for example, may be used for both communication-related functions, such as entering a text message for transmission over a communication network, and device-resident functions such as a calculator or task list.

[0204] Operating system software used by the microprocessor **2238** is preferably stored in a persistent store such as flash memory **2224**, which may instead be a read-only memory (ROM) or similar storage element (not shown). Those skilled in the art will appreciate that the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile memory such as RAM **2226**. Received communication signals may also be stored in RAM **2226**.

[0205] As shown, flash memory **2224** can be segregated into different areas for both computer programs **2258** and program data storage **2250**, **2252**, **2254** and **2256**. These different storage types indicate that each program can allocate a portion of flash memory **2224** for their own data storage requirements. Microprocessor **2238**, in addition to its operating system functions, preferably enables execution of software applications on the mobile station. A predetermined set of applications that control basic operations, including at least data and voice communication applications for example, will normally be installed on mobile station **2200** during manufacturing. Other applications could be installed subsequently or dynamically.

[0206] A preferred software application may be a personal information manager (PIM) application having the ability to organize and manage data items relating to the user of the mobile station such as, but not limited to, e-mail, calendar events, voice mails, appointments, and task items. Naturally, one or more memory stores would be available on the mobile station to facilitate storage of PIM data items. Such PIM application would preferably have the ability to send and receive data items, via the wireless network **2219**. In a preferred embodiment, the PIM data items are seamlessly integrated, synchronized and updated, via the wireless network **2219**, with the mobile station user's corresponding data items stored or associated with a host computer system. Further applications may also be loaded onto the mobile station **2200** through the network **2219**, an auxiliary I/O subsystem **2228**, serial port **2230**, short-range communications subsystem **2240** or any other suitable subsystem **2242**, and installed by a user in the RAM **2226** or preferably a non-volatile

store (not shown) for execution by the microprocessor **2238**. Such flexibility in application installation increases the functionality of the device and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile station **2200**.

[0207] In a data communication mode, a received signal such as a text message or web page download will be processed by the communication subsystem **2211** and input to the microprocessor **2238**, which preferably further processes the received signal for output to the display **2222**, or alternatively to an auxiliary I/O device **2228**. A push client **2260**, which could be equivalent to push clients **140** and **510**, could also process the input.

[0208] A user of mobile station **2200** may also compose data items such as email messages for example, using the keyboard **2232**, which is preferably a complete alphanumeric keyboard or telephone-type keypad, in conjunction with the display **2222** and possibly an auxiliary I/O device **2228**. Such composed items may then be , transmitted over a communication network through the communication subsystem **2211**.

[0209] For voice communications, overall operation of mobile station **2200** is similar, except that received signals would preferably be output to a speaker **2234** and signals for transmission would be generated by a microphone **2236**. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on mobile station **2200**. Although voice or audio signal output is preferably accomplished primarily through the speaker **2234**, display **2222** may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information for example.

[0210] Serial port **2230** in **Figure 22**, would normally be implemented in a personal digital assistant (PDA)-type mobile station for which synchronization with a user's desktop computer (not shown) may be desirable, but is an optional device component. Such a port **2230** would enable a user to set preferences through an external device or software application and would extend the capabilities of mobile station **2200** by providing for information or software downloads to mobile station **2200** other than through a wireless communication network. The alternate download path may for example be used to load an encryption key onto the device through a direct and thus reliable and trusted connection to thereby enable secure device communication. As will be appreciated by those skilled in the art, serial port **2230** can further be used to connect the mobile device to a computer to act as a modem.

[0211] Other communications subsystems **2240**, such as a short-range communications subsystem, is a further optional component which may provide for communication between mobile station **2200** and different systems or devices, which need not necessarily be similar devices. For example, the subsystem **2240** may include an infrared device and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices.

[0212] The embodiments described herein are examples of structures, systems or methods having elements corresponding to elements of the techniques of this application. This written description may enable those skilled in the art to make and use embodiments having alternative elements that likewise correspond to the elements of the techniques of this application. The intended scope of the techniques of this application thus includes other structures, systems or methods that do not differ from the techniques of this application as described herein, and further includes other structures, systems or methods with insubstantial differences from the techniques of this application as described herein.

Claims

1. A push proxy (410) for use in a generic dynamic content delivery system comprising:

a content provider registration service provider interface (420), said service provider interface (420) adapted to register content providers (412) (412) with said push proxy (410) and to further receive channel metadata for the content providers (412);

a channel metadata repository (470), said channel metadata repository (470) adapted to store said channel metadata received from the content providers (412);

a content metadata extractor and cache module (450), said content metadata extractor and cache module (450) being adapted to extract metadata for said push proxy (410) from a content and metadata envelope received from the content providers (412), said content metadata extractor and cache module (450) further adapted to cache said metadata on said push proxy (410);

a content fragmentation module (464), said content fragmentation module (464) adapted to break a content and metadata envelope into segments;

a deferred retrieval message store module (452), said deferred retrieval message store module (452) adapted to store a content envelope or one or more segments from said content fragmentation module (464);

a content expiry and replacement module (466), said content expiry and replacement module (466) adapted to expire content stored in the deferred retrieval message store module (452) or to replace content stored in the

- deferred retrieval message store module (452);
a content dependencies module (462), said content dependencies module (462) adapted to provide selection of push clients (510) to advertise a service to;
a push scheduler (454), said push scheduler (454) adapted to schedule the pushing of a content envelope stored in the deferred retrieval message store module (452); and
a subscription and rules module (460), said subscription and rules module (460) adapted to maintain a subscription between an application and the content provider (412) and maintain a list of rules for the subscription.
2. The push proxy (410) of claim 1, further comprising push agents (444) to push content and metadata envelopes to a push client (510).
3. The push proxy (410) of claim 1 or claim 2, further comprising a flow control management module (442), the flow control management module (442) adapted to receive flow control messages from the push client (510) and start or stop pushing content and metadata envelopes.
4. The push proxy (410) of any one of claims 1 to 3, further comprising message brokers and delivery queues (440) to store and manage content and metadata envelopes.
5. A push client (510) for use in a dynamic content delivery architecture, the push client comprising:
- an application registration application provider interface (514) adapted to register applications (512) to said push client and further adapted to receive an application manifest (918) for said applications, said application manifest (918) containing channel metadata;
a channel metadata repository (570) adapted to store channel metadata received from said application (512);
communication means, such communication means adapted to receive a content and metadata envelope from a push proxy (410);
content metadata extractor and cache module (550), said content metadata extractor and cache module (550) being adapted to extract metadata for said push client from said content and metadata envelope and further being adapted to cache said metadata on said push client;
a deferred retrieval manager (552) adapted to schedule retrieval of content from the push proxy (410) not yet received by the push client (510);
a content dependencies module (564) adapted to reconstitute content previously broken into segments;
a content expiry and replacement module (566), said content expiry and replacement module (566) adapted to expire content stored at said push client or to replace content stored at the push client;
an update notification block (562), said update notification block adapted to work with said applications (512) to notify the applications that new content is waiting for them;
a subscription management block (560), said subscription management block (560) adapted to manage subscriptions between the application and a content provider;
a pull broker (554) adapted to pull content when required by the push client, said pull broker being driven by said deferred retrieval manager (552),
- wherein said push client is adapted to register generic applications and receive generic content type from the content provider.
6. The push client (510) of claim 5, further comprising push agents (544) to receive content and metadata envelopes from the push proxy (410).
7. The push client (510) of claim 5 or claims 6, further comprising a flow control management module (542), the flow control management module (542) adapted to send flow control messages to the push proxy (410) to start or stop pushing content and metadata envelopes.
8. The push client (510) of any one of claims 5 to 7, further comprising message brokers and delivery queues (540) to store and manage content and metadata envelopes.
9. The push client (510) of any one of claims 5 to 8, wherein said push client further comprises a background update processing module (575) adapted to perform background updates for applications not connected with said push client.
10. The push client (510) of any one of claims 5 to 9, wherein the update notification block (562) is adapted to store

content for said applications in predetermined locations.

11. The push client (510) of claim 10, wherein the update notification block (562) is adapted to send a message to the client application that data has been stored in the predetermined locations.
12. The push client (510) of any one of claims 5 to 11, wherein the update notification block (562) is adapted to send the content and metadata envelope to the applications.
13. A method of pushing generic dynamic content via a push proxy (410) of a generic dynamic content delivery system, the method comprising:
 - obtaining a service manifest (962) at the push proxy (410), the services manifest (962) corresponding to a dynamic content push service provided by a service provider (120);
 - registering a content provider (412) with the generic dynamic content delivery system by registering the content provider with the push proxy (410) having a content provider registration interface (420) to receive channel metadata from the content provider;
 - storing said channel metadata in a channel metadata repository (470) associated with the push proxy (410);
 - receiving a content and metadata envelope at the push proxy (410) from the content provider; and
 - processing the content and metadata envelope in accordance with the channel metadata.
14. A method as claimed in claim 13 further comprising:
 - extracting metadata for said push proxy (410) from said content and metadata envelope; and
 - processing said content and metadata envelope in accordance with said extracted metadata.
15. A method as claimed in claim 14 further comprising processing the content of said content and metadata envelope in accordance with said extracted metadata.
16. A method as claimed in any one of claims 13 to 15 further comprising fragmenting a content and metadata envelope into segments.
17. A method as claimed in claim 16 further comprising storing one of content, a content segment, a content and metadata envelope, and a content and metadata envelope segment in a deferred retrieval message store (452).
18. A method as claimed in claim 17 further comprising any of: expiring time sensitive content stored in the deferred retrieval message store (452); replacing content stored in the deferred retrieval message store (452) with updated content; or scheduling the pushing of the contents said deferred retrieval message store (452).
19. A method as claimed in any one of claims 13 to 15 further comprising determining a selection of push clients (510) from content dependencies.
20. A method as claimed in claims 19 further comprising any of: providing the selection of push clients (510) to advertise a service thereto; or maintaining a subscription between an application and the content provider (412).
21. A method as claimed in claim 20 further comprising maintaining a list of rules for the subscription.
22. A method as claimed in any one of claims 13 to 15, 16, 17 or 18 further comprising pushing said content and metadata envelope to a push client (510).
23. A method as claimed in claims 22 further comprising:
 - receiving flow control messages from the push client (510); and
 - selectively pushing said content and metadata envelope to the push client as directed via the flow control messages.
24. A method as claimed in any one of claims 13, 16 or 17 further comprising storing content and metadata in a plurality of delivery queues. (440).

25. A method as claimed in claim 24 further comprising managing content and metadata stored in the plurality of delivery queues by employing at least one message broker (440).
- 5 26. A method of pushing generic dynamic content via a push client (510) of a generic dynamic content delivery system, the method comprising:
- obtaining an application manifest (962) at a push client, the application manifest corresponding to an application (512) processing dynamic content pushed thereto;
 10 registering the application with the generic dynamic content delivery system by registering the application with the push client having an application registration interface (514), said application manifest containing channel metadata;
 storing said channel metadata in a channel metadata repository (570) associated with the push client;
 receiving a content and metadata envelope at the push client via a push proxy (410); and
 15 processing the content and metadata envelope in accordance with the channel metadata.
27. A method as claimed in claim 26 further comprising:
- extracting metadata for said push client from said content and metadata envelope; and
 20 processing said content and metadata envelope in accordance with said extracted metadata.
28. A method as claimed in claim 27 further comprising processing the content of said content and metadata envelope in accordance with said extracted metadata.
29. A method as claimed in any one of claims 26 to 28 further comprising scheduling retrieval of content yet to be received by the push client (510) via said push proxy (410).
- 25 30. A method as claimed in claim 29 further comprising pulling content as directed by a deferred retrieval manager (552) performing the scheduling of said retrieval of content.
- 30 31. A method as claimed in claim 30 further comprising storing one of content, a content segment, a content and metadata envelope, and a content and metadata envelope segment at the push client (510).
32. A method as claimed in claim 31 further comprising any of: expiring time sensitive content stored at said push client (510); replacing content stored at said push client with updated content; or reconstituting content previously broken
 35 into segments based on content dependencies.
33. A method as claimed in claim 26 further comprising selectively sending flow control messages to the push proxy (410) to push said content and metadata envelope to the push client (510).
- 40 34. A method as claimed in any one of claims 26, 31 or 32 further comprising storing content and metadata in a plurality of delivery queues (540).
35. A method as claimed in claim 34 further comprising managing content and metadata stored in the plurality of delivery queues by employing at least one message broker (540).
- 45

Patentansprüche

- 50 1. Push-Proxy (410) zur Verwendung in einem System zur Zustellung von generischen dynamischen Inhalten, umfassend:
- eine Diensteanbieter-Schnittstelle (420) für die Inthalteanbieter-Registrierung, wobei die Diensteanbieter-Schnittstelle (420) dafür ausgelegt ist, Inthalteanbieter (412) bei dem Push-Proxy (410) zu registrieren und
 55 ferner Kanal-Metadaten für die Inthalteanbieter (412) zu empfangen;
 ein Kanal-Metadaten-Repository (470), wobei das Kanal-Metadaten-Repository (470) dafür ausgelegt ist, die von den Inthalteanbietern (412) empfangenen Kanal-Metadaten zu speichern;
 ein Modul zum Extrahieren und Zwischenspeichern von Inthalte-Metadaten (450), wobei das Modul zum Extrahieren und Zwischenspeichern von Inthalte-Metadaten (450) dafür ausgelegt ist, Metadaten für den Push-Proxy

- (410) aus einer Inhalte- und Metadaten-Envelope zu extrahieren, die von den Inhaltenanbietern (412) empfangen wurde, wobei das Modul zum Extrahieren und Zwischenspeichern von Inhalte-Metadaten (450) ferner dafür ausgelegt ist, die Metadaten auf dem Push-Proxy (410) zwischenzuspeichern;
 ein Modul zum Fragmentieren von Inhalten (464), wobei das Modul zum Fragmentieren von Inhalten (464) dafür ausgelegt ist, eine Inhalte- und Metadaten-Envelope in Segmente aufzugliedern;
 ein Modul zum Speichern von Nachrichten für verzögerten Abruf (452), wobei das Modul zum Speichern von Nachrichten für verzögerten Abruf (452) dafür ausgelegt ist, eine Inhalte-Envelope oder ein oder mehrere Segment(e) von dem Modul zum Fragmentieren von Inhalten (464) zu speichern;
 ein Modul für Verfall und Austausch von Inhalten (466), wobei das Modul für Verfall und Austausch von Inhalten (466) dafür ausgelegt ist, in dem Modul zum Speichern von Nachrichten für verzögerten Abruf (452) gespeicherte Inhalte verfallen zu lassen oder in dem Modul zum Speichern von Nachrichten für verzögerten Abruf (452) gespeicherte Inhalte auszutauschen;
 ein Modul für Inhalte-Abhängigkeiten (462), wobei das Modul für Inhalte-Abhängigkeiten (462) dafür ausgelegt ist, eine Auswahl von Push-Clients (510) bereitzustellen, bei denen für einen Dienst geworben werden soll;
 einen Push-Planer (454), wobei der Push-Planer (454) dafür ausgelegt ist, die Auslieferung einer in dem Modul zum Speichern von Nachrichten für verzögerten Abruf (452) gespeicherten Inhalte-Envelope zu planen; und
 ein Subskriptions- und Regelmodul (460), wobei das Subskriptions- und Regelmodul (460) dafür ausgelegt ist, eine Subskription zwischen einer Anwendung und dem Inhaltenanbieter (412) sowie eine Liste der Regeln für die Subskription zu verwalten.
2. Push-Proxy (410) nach Anspruch 1, ferner umfassend Push-Agenten (444), um Inhalte- und Metadaten-Envelopes an einen Push-Client (510) auszuliefern.
3. Push-Proxy (410) nach Anspruch 1 oder Anspruch 2, ferner umfassend ein Flusssteuerungs-Management-Modul (442), wobei das Flusssteuerungs-Management-Modul (442) dafür ausgelegt ist, Flusssteuerungsnachrichten von dem Push-Client (510) zu empfangen und die Auslieferung von Inhalte- und Metadaten-Envelopes zu starten oder zu beenden.
4. Push-Proxy (410) nach Anspruch 1 bis 3, ferner umfassend Message-Broker und Zustell-Warteschlangen (440) zum Speichern und Verwalten von Inhalte- und Metadaten-Envelopes.
5. Push-Client (510) zur Verwendung in einer Architektur zur Zustellung von dynamischen Inhalten, wobei der Push-Client umfasst:
- eine Anwendungsanbieter-Schnittstelle zur Anwendungsregistrierung (514), die dafür ausgelegt ist, Anwendungen (512) bei dem Push-Client zu registrieren, und ferner dafür ausgelegt ist, ein Anwendungsmanifest (918) für die Anwendungen zu empfangen, wobei das Anwendungsmanifest (918) Kanal-Metadaten enthält;
 ein Kanal-Metadaten-Repository (570), das dafür ausgelegt ist, von der Anwendung (512) empfangene Kanal-Metadaten zu speichern,
 Kommunikationsmittel, wobei derartige Kommunikationsmittel dafür ausgelegt sind, eine Inhalte- und Metadaten-Envelope von einem Push-Proxy (410) zu empfangen;
 ein Modul zum Extrahieren und Zwischenspeichern von Inhalte-Metadaten (550), wobei das Modul zum Extrahieren und Zwischenspeichern von Inhalte-Metadaten (550) dafür ausgelegt ist, Metadaten für den Push-Client aus der Inhalt- und Metadaten-Envelope zu extrahieren, und ferner dafür ausgelegt ist, die Metadaten auf dem Push-Client zwischenzuspeichern;
 einen Manager für verzögerten Abruf (552), der dafür ausgelegt ist, den Abruf von Inhalten, die der Push-Client (510) bisher nicht empfangen hat, von einem Push-Proxy (410) zu planen;
 ein Modul für Inhalte-Abhängigkeiten (564), das dafür ausgelegt ist, zuvor in Segmente untergliederte Inhalte wieder zusammenzusetzen;
 ein Modul für Verfall und Austausch von Inhalten (566), wobei das Modul für Verfall und Austausch von Inhalten (566) dafür ausgelegt ist, auf dem Push-Client gespeicherte Inhalte verfallen zu lassen bzw. auf dem Push-Client gespeicherte Inhalte auszutauschen;
 einen Update-Benachrichtigungsblock (562), wobei der Update-Benachrichtigungsblock (562) dafür ausgelegt ist, mit den Anwendungen (512) zusammenzuarbeiten, um die Anwendungen zu benachrichtigen, dass neue Inhalte für sie bereitstehen;
 einen Subskriptions-Management-Block (560), wobei der Subskriptions-Management-Block (560) dafür ausgelegt ist, Subskriptionen zwischen der Anwendung und einem Inhaltenanbieter zu verwalten;
 einen Pull-Broker (554), der dafür ausgelegt ist, Inhalte abzurufen, wenn der Push-Client dies fordert, wobei

EP 1 853 044 B1

der Pull-Broker von dem Manager für verzögerten Abruf (552) gesteuert wird,

wobei der Push-Client dafür ausgelegt ist, generische Anwendungen zu registrieren und Inhalte generischer Art von dem Inhaltenanbieter zu empfangen.

5

6. Push-Client (510) nach Anspruch 5, ferner umfassend Push-Agenten (544), um Inhalte- und Metadaten-Envelopes von dem Push-Proxy (410) zu empfangen.

10

7. Push-Client (510) nach Anspruch 5 oder 6, ferner umfassend ein Flusssteuerungs-Management-Modul (542), wobei das Flusssteuerungs-Management-Modul (542) dafür ausgelegt ist, Flusssteuerungsnachrichten an den Push-Proxy (410) zu senden, um die Auslieferung von Inhalte- und Metadaten-Envelopes zu starten bzw. zu beenden.

15

8. Push-Client (510) nach einem der Ansprüche 5 bis 7, ferner umfassend Message-Broker- und Zustell-Warteschlangen (540) zum Speichern und Verwalten von Inhalte- und Metadaten-Envelopes.

9. Push-Client (510) nach einem der Ansprüche 5 bis 8, wobei der Push-Client ferner ein Modul für die Update-Verarbeitung im Hintergrund (575) umfasst, das dafür ausgelegt ist, im Hintergrund Updates für Anwendungen auszuführen, die nicht mit dem Push-Client verbunden sind.

20

10. Push-Client (510) nach einem der Ansprüche 5 bis 9, wobei der Update-Benachrichtigungsblock (562) dafür ausgelegt ist, Inhalte für die Anwendungen an vorab definierten Speicherorten abzulegen.

25

11. Push-Client (510) nach Anspruch 10, wobei der Update-Benachrichtigungsblock (562) dafür ausgelegt ist, eine Nachricht an die Client-Anwendung zu senden, dass Daten an den vorab definierten Speicherorten abgelegt wurden.

12. Push-Client (510) nach einem der Ansprüche 5 bis 11, wobei der Update-Benachrichtigungsblock (562) dafür ausgelegt ist, die Inhalte- und Metadaten-Envelope an die Anwendungen zu senden.

30

13. Verfahren für die Auslieferung generischer dynamischer Inhalte über einen Push-Proxy (410) eines Systems zur Zustellung von generischen dynamischen Inhalten, umfassend:

35

Empfangen eines Dienstmanifests (962) am Push-Proxy (410), wobei das Dienstmanifest (962) einem Push-Dienst mit dynamischen Inhalten entspricht, der von einem Diensteanbieter (120) bereitgestellt wird;

Registrieren eines Inhaltenanbieters (412) bei dem System zur Zustellung von generischen dynamischen Inhalten, indem der Inhaltenanbieter bei dem Push-Proxy (410) registriert wird, welcher eine Schnittstelle für die Inhaltenanbieter-Registrierung (420) besitzt, um Kanal-Metadaten von dem Inhaltenanbieter zu empfangen; Speichern der Kanal-Metadaten in einem Kanal-Metadaten-Repository (470), das dem Push-Proxy (410) zugeordnet ist;

40

Empfangen einer Inhalte- und Metadaten-Envelope von dem Inhaltenanbieter am Push-Proxy (410); und Verarbeiten der Inhalte- und Metadaten-Envelope entsprechend den Kanal-Metadaten.

14. Verfahren nach Anspruch 13, ferner umfassend:

45

Extrahieren von Metadaten für den Push-Proxy (410) aus der Inhalte- und Metadaten-Envelope; und Verarbeiten der Inhalte- und Metadaten-Envelope entsprechend den extrahierten Metadaten.

15. Verfahren nach Anspruch 14, ferner umfassend das Verarbeiten der Inhalte aus der Inhalte- und Metadaten-Envelope entsprechend den extrahierten Metadaten.

50

16. Verfahren nach einem der Ansprüche 13 bis 15, ferner umfassend das Fragmentieren einer Inhalte- und Metadaten-Envelope in Segmente.

55

17. Verfahren nach Anspruch 16, ferner umfassend das Speichern entweder der Inhalte oder eines Inhaltssegments oder einer Inhalte- und Metadaten-Envelope oder eines Segments einer Inhalte- und Metadaten-Envelope in einem Modul zum Speichern von Nachrichten für verzögerten Abruf (452).

18. Verfahren nach Anspruch 17, ferner umfassend ein beliebiges von: Verfallenlassen zeitkritischer Inhalte, die in dem Modul zum Speichern von Nachrichten für verzögerten Abruf (452) gespeichert sind; Austauschen von Inhalten,

EP 1 853 044 B1

die in dem Modul zum Speichern von Nachrichten für verzögerten Abruf (452) gespeichert sind, durch aktualisierte Inhalte; oder Planen der Auslieferung der Inhalte in dem Modul zum Speichern von Nachrichten für verzögerten Abruf (452).

- 5 **19.** Verfahren nach einem der Ansprüche 13 bis 15, ferner umfassend das Bestimmen einer Auswahl von Push-Clients (510) anhand von Abhängigkeiten der Inhalte.
- 10 **20.** Verfahren nach Anspruch 19, ferner umfassend ein beliebiges von: Bereitstellen der Auswahl von Push-Clients (510), um bei ihnen für einen Dienst zu werben; oder Verwalten einer Subskription zwischen einer Anwendung und dem Inhalteanbieter (412).
- 15 **21.** Verfahren nach Anspruch 20, ferner umfassend das Verwalten einer Liste von Regeln für die Subskription.
- 15 **22.** Verfahren nach einem der Ansprüche 13 bis 15, 16, 17 oder 18, ferner umfassend das Ausliefern der Inhalte- und Metadaten-Envelope an einen Push-Client (510).
- 20 **23.** Verfahren nach Anspruch 22, ferner umfassend:
Empfangen von Flusssteuerungs-Nachrichten von dem Push-Client (510); und
selektives Ausliefern der Inhalte- und Metadaten-Envelope an den Push-Client wie durch die Flusssteuerungs-Nachrichten vorgegeben.
- 25 **24.** Verfahren nach einem der Ansprüche 13, 16 oder 17, ferner umfassend das Speichern der Inhalte und Metadaten in einer Mehrzahl von Zustell-Warteschlangen (440).
- 25 **25.** Verfahren nach Anspruch 24, ferner umfassend das Verwalten der Inhalte und Metadaten, die in der Mehrzahl von Zustell-Warteschlangen gespeichert sind, durch Einsatz mindestens eines Message-Brokers (440).
- 30 **26.** Verfahren für die Auslieferung generischer dynamischer Inhalte über einen Push-Client (510) eines Systems zur Zustellung von generischen dynamischen Inhalten, umfassend:
Empfangen eines Anwendungsmanifests (962) an einem Push-Client, wobei das Anwendungsmanifest einer Anwendung (512) entspricht, die an sie ausgelieferte dynamische Inhalte verarbeitet;
Registrieren der Anwendung bei dem System zur Zustellung von generischen dynamischen Inhalten, indem
35 die Anwendung bei dem Push-Client registriert wird, welcher eine Schnittstelle für die Anwendungsregistrierung (514) besitzt, wobei das Anwendungsmanifest Kanal-Metadaten enthält;
Speichern der Kanal-Metadaten in einem Kanal-Metadaten-Repository (570), das dem Push-Client zugeordnet ist;
Empfangen einer Inhalte- und Metadaten-Envelope am Push-Client über einen Push-Proxy (410); und
40 Verarbeiten der Inhalte- und Metadaten-Envelope entsprechend den Kanal-Metadaten.
- 45 **27.** Verfahren nach Anspruch 26, ferner umfassend:
Extrahieren von Metadaten für den Push-Client aus der Inhalte- und Metadaten-Envelope; und
Verarbeiten der Inhalte- und Metadaten-Envelope entsprechend den extrahierten Metadaten.
- 50 **28.** Verfahren nach Anspruch 27, ferner umfassend das Verarbeiten der Inhalte aus der Inhalte- und Metadaten-Envelope entsprechend den extrahierten Metadaten.
- 50 **29.** Verfahren nach einem der Ansprüche 26 bis 28, ferner umfassend das Planen des Abrufens von Inhalten, die von dem Push-Client (510) noch empfangen werden müssen, über den Push-Proxy (410).
- 55 **30.** Verfahren nach Anspruch 29, ferner umfassend das Abrufen von Inhalten gemäß Vorgabe durch einen Manager für verzögerten Abruf (552), der das Abrufen von Inhalten plant.
- 55 **31.** Verfahren nach Anspruch 30, ferner umfassend das Speichern entweder der Inhalte oder eines Inhaltssegments oder einer Inhalte- und Metadaten-Envelope oder eines Segments einer Inhalte- und Metadaten-Envelope am Push-Client (510).

EP 1 853 044 B1

- 5
32. Verfahren nach Anspruch 31, ferner umfassend ein beliebiges von: Verfallenlassen zeitkritischer Inhalte, die an dem Push-Client (510) gespeichert sind; Austauschen von Inhalten, die an dem Push-Client gespeichert sind, durch aktualisierte Inhalte; oder Zusammensetzen von zuvor in Segmente untergliederten Inhalten auf Basis von Abhängigkeiten der Inhalte.
- 10
33. Verfahren nach Anspruch 26, ferner umfassend das selektive Senden von Flusssteuerungs-Nachrichten an den Push-Proxy (410), um die Inhalte- und Metadaten-Envelope an den Push-Client (510) auszuliefern.
34. Verfahren nach einem der Ansprüche 26, 31 oder 32, ferner umfassend das Speichern der Inhalte und Metadaten in einer Mehrzahl von Zustell-Warteschlangen (540).
- 15
35. Verfahren nach Anspruch 34, ferner umfassend das Verwalten der Inhalte und Metadaten, die in der Mehrzahl von Zustell-Warteschlangen gespeichert sind, durch Einsatz mindestens eines Message-Brokers (540).

Revendications

- 20
1. Un proxy push (410) destiné à une utilisation dans un système de remise de contenus dynamiques génériques comprenant :
- 25
- une interface de fournisseur de services d'enregistrement de fournisseur de contenus (420), ladite interface de fournisseur de services (420) étant adaptée de façon à enregistrer des fournisseurs de contenus (412) auprès dudit proxy push (410) et de façon à recevoir en outre des métadonnées de canal pour les fournisseurs de contenus (412),
- 30
- un entrepôt de métadonnées de canal (470), ledit entrepôt de métadonnées de canal (470) étant adapté de façon à conserver en mémoire lesdites métadonnées de canal reçues des fournisseurs de contenus (412),
- 35
- un module d'extracteur de métadonnées de contenu et de mémoire tampon (450), ledit module d'extracteur de métadonnées de contenu et de mémoire tampon (450) étant adapté de façon à extraire des métadonnées pour ledit proxy push (410) d'une enveloppe de métadonnées et de contenus reçue des fournisseurs de contenus (412), ledit module d'extracteur de métadonnées de contenu et de mémoire tampon (450) étant adapté en outre de façon à placer en mémoire tampon lesdites métadonnées sur ledit proxy push (410),
- 40
- un module de fragmentation de contenus (464), ledit module de fragmentation de contenus (464) étant adapté de façon à diviser une enveloppe de métadonnées et de contenus en segments,
- 45
- un module d'espace mémoire de messages à récupération différée (452), ledit module d'espace mémoire de messages à récupération différée (452) étant adapté de façon à conserver en mémoire une enveloppe de contenus ou un ou plusieurs segments provenant dudit module de fragmentation de contenus (464),
- un module de remplacement et d'expiration de contenus (466), ledit module de remplacement et d'expiration de contenus (466) étant adapté de façon à faire expirer les contenus conservés en mémoire dans le module d'espace mémoire de messages à récupération différée (452) ou de façon à remplacer les contenus conservés en mémoire dans le module d'espace mémoire de messages à récupération différée (452),
- 50
- un module de dépendances de contenus (462), ledit module de dépendances de contenus (462) étant adapté de façon à fournir une sélection de clients push (510) auxquels annoncer un service,
- 55
- un ordonnanceur push (454), ledit ordonnanceur push (454) étant adapté de façon à ordonnancer l'envoi d'une enveloppe de contenus conservée en mémoire dans le module d'espace mémoire de messages à récupération différée (452), et
- un module de règles et d'abonnement (460), ledit module de règles et d'abonnement (460) étant adapté de façon à entretenir un abonnement entre une application et le fournisseur de contenus (412) et à entretenir une liste de règles relatives à l'abonnement.
2. Le proxy push (410) selon la revendication 1, comprenant en outre des agents push (444) chargés d'envoyer des enveloppes de métadonnées et de contenus à un client push (510).
3. Le proxy push (410) selon la revendication 1 ou 2, comprenant en outre un module de gestion de régulation du flux (442), le module de gestion de régulation du flux (442) étant adapté de façon à recevoir des messages de régulation de flux du client push (510) et de façon à démarrer ou suspendre l'envoi d'enveloppes de métadonnées et de contenus.
4. Le proxy push (410) selon l'une quelconque des revendications 1 à 3, comprenant en outre des courtiers de messages

et des files d'attente de remise (440) destinés à conserver en mémoire et à gérer des enveloppes de métadonnées et de contenus.

5. Un client push (510) destiné à une utilisation dans une architecture de remise de contenus dynamiques, le client push comprenant :

une interface de fournisseur d'applications d'enregistrement d'applications (514) adaptée de façon à enregistrer des applications (512) auprès dudit client push et adaptée en outre de façon à recevoir un descriptif d'application (918) pour lesdites applications, ledit descriptif d'application (918) contenant des métadonnées de canal, un entrepôt de métadonnées de canal (570) adapté de façon à conserver en mémoire des métadonnées de canal reçues de ladite application (512), un moyen de communication, ce moyen de communication étant adapté de façon à recevoir une enveloppe de métadonnées et de contenus d'un proxy push (410), un module d'extracteur de métadonnées de contenu et de mémoire tampon (550), ledit module d'extracteur de métadonnées de contenu et de mémoire tampon (450) étant adapté de façon à extraire des métadonnées pour ledit client push de ladite enveloppe de métadonnées et de contenus et étant adapté en outre de façon à placer en mémoire tampon lesdites métadonnées sur ledit client push, un gestionnaire de récupération différée (552) adapté de façon à ordonnancer la récupération de contenus du proxy push (410) non encore reçus par le client push (510), un module de dépendances de contenus (564) adapté de façon à reconstituer des contenus antérieurement divisés en segments, un module de remplacement et d'expiration de contenus (566), ledit module de remplacement et d'expiration de contenus (566) étant adapté de façon à faire expirer des contenus conservés en mémoire sur ledit client push ou de façon à remplacer des contenus conservés en mémoire sur le client push, un bloc de notification de mise à jour (562), ledit bloc de notification de mise à jour étant adapté de façon à travailler avec lesdites applications (512) de façon à notifier les applications que de nouveaux contenus sont en attente à leur attention, un bloc de gestion des abonnements (560), ledit bloc de gestion des abonnements (560) étant adapté de façon à gérer des abonnements entre l'application et un fournisseur de contenus, un courtier de transfert de contenus (554) adapté de façon à transférer des contenus lorsqu'exigé par le client push, ledit courtier de transfert de contenus (554) étant piloté par ledit gestionnaire de récupération différée (552),

où ledit client push est adapté de façon à enregistrer des applications génériques et à recevoir des contenus de type générique du fournisseur de contenus.

6. Le client push (510) selon la revendication 5, comprenant en outre des agents push (544) destinés à recevoir des enveloppes de métadonnées et de contenus du proxy push (410).
7. Le client push (510) selon la revendication 5 ou 6, comprenant en outre un module de gestion de régulation du flux (542), le module de gestion de régulation du flux (442) étant adapté de façon à envoyer des messages de régulation de flux au proxy push (410) de façon à démarrer ou suspendre l'envoi d'enveloppes de métadonnées et de contenus.
8. Le client push (510) selon l'une quelconque des revendications 5 à 7, comprenant en outre des courtiers de messages et des files d'attente de remise (540) destinés à conserver en mémoire et à gérer des enveloppes de métadonnées et de contenus.
9. Le client push (510) selon l'une quelconque des revendications 5 à 8, où ledit client push comprend en outre un module de traitement de mise à jour en arrière-plan (575) adapté de façon à exécuter des mises à jour en arrière-plan pour des applications non connectées audit client push.
10. Le client push (510) selon l'une quelconque des revendications 5 à 9, où le bloc de notification de mise à jour (562) est adapté de façon à conserver en mémoire des contenus pour lesdites applications dans des emplacements prédéterminés.
11. Le client push (510) selon la revendication 10, où le bloc de notification de mise à jour (562) est adapté de façon à envoyer un message à l'application client signalant que des données ont été placées en mémoire dans les emplacements prédéterminés.

EP 1 853 044 B1

12. Le client push (510) selon l'une quelconque des revendications 5 à 11, où le bloc de notification de mise à jour (562) est adapté de façon à envoyer l'enveloppe de métadonnées et de contenus aux applications.
- 5 13. Un procédé d'envoi de contenus dynamiques génériques par l'intermédiaire d'un proxy push (410) d'un système de remise de contenus dynamiques génériques, le procédé comprenant :
- 10 l'obtention d'un descriptif de service (962) auprès du proxy push (410), le descriptif de service (962) correspondant à un service d'envoi de contenus dynamiques fourni par un fournisseur de services (120),
l'enregistrement d'un fournisseur de contenus (412) auprès du système de remise de contenus dynamiques
15 génériques par l'enregistrement du fournisseur de contenus auprès du proxy push (410) possédant une interface d'enregistrement de fournisseur de contenus (420) de façon à recevoir des métadonnées de canal du fournisseur de contenus,
la mise en mémoire desdites métadonnées de canal dans un entrepôt de métadonnées de canal (470) associé au proxy push (410),
15 la réception d'une enveloppe de métadonnées et de contenus sur le proxy push (410) provenant du fournisseur de contenus, et
le traitement de l'enveloppe de métadonnées et de contenus selon les métadonnées de canal.
- 20 14. Un procédé selon la revendication 13 comprenant en outre :
- l'extraction de métadonnées pour ledit proxy push (410) de ladite enveloppe de métadonnées et de contenus, et le traitement de ladite enveloppe de métadonnées et de contenus selon lesdites métadonnées extraites.
- 25 15. Un procédé selon la revendication 14 comprenant en outre le traitement des contenus de ladite enveloppe de métadonnées et de contenus selon lesdites métadonnées extraites.
- 30 16. Un procédé selon l'une quelconque des revendications 13 à 15 comprenant en outre la fragmentation d'une enveloppe de métadonnées et de contenus en segments.
- 35 17. Un procédé selon la revendication 16 comprenant en outre la mise en mémoire d'un élément parmi les éléments suivants : un contenu, un segment de contenu, une enveloppe de métadonnées et de contenus ou un segment d'enveloppe de métadonnées et de contenus dans un espace mémoire de messages à récupération différée (452).
- 40 18. Un procédé selon la revendication 17 comprenant en outre l'une quelconque des opérations suivantes : l'expiration de contenus sensibles au temps conservés en mémoire dans l'espace mémoire de messages à récupération différée (452), le remplacement des contenus conservés en mémoire dans l'espace mémoire de messages à récupération différée (452) par des contenus mis à jour, ou l'ordonnancement de la transmission des contenus de l'espace mémoire de messages à récupération différée (452).
- 45 19. Un procédé selon l'une quelconque des revendications 13 à 15 comprenant en outre la détermination d'une sélection de clients push (510) à partir de dépendances de contenus.
20. Un procédé selon la revendication 19 comprenant en outre l'une quelconque des opérations suivantes : la fourniture de la sélection de clients push (510) afin d'annoncer un service à ces derniers ou l'entretien d'un abonnement entre une application et le fournisseur de contenus (412).
- 50 21. Un procédé selon la revendication 20 comprenant en outre l'entretien d'une liste de règles relatives à l'abonnement.
22. Un procédé selon l'une quelconque des revendications 13 à 15, 16, 17 ou 18 comprenant en outre la transmission de ladite enveloppe de métadonnées et de contenus à un client push (510).
- 55 23. Un procédé selon la revendication 22 comprenant en outre :
- la réception de messages de régulation de flux du client push (510), et
la transmission sélective de ladite enveloppe de métadonnées et de contenus au client push comme indiqué par les messages de régulation de flux.
24. Un procédé selon l'une quelconque des revendications 13, 16 ou 17 comprenant en outre la mise en mémoire des

EP 1 853 044 B1

contenus et des métadonnées dans une pluralité de files d'attente de remise (440).

- 5
25. Un procédé selon la revendication 24 comprenant en outre la gestion des contenus et des métadonnées conservés en mémoire dans la pluralité de files d'attente de remise en utilisant au moins un courtier de messages (440).
- 10
26. Un procédé d'envoi de contenus dynamiques génériques par l'intermédiaire d'un client push (510) d'un système de remise de contenus dynamiques génériques, le procédé comprenant :
- 15
- l'obtention d'un descriptif d'application (962) auprès d'un client push, le descriptif d'application correspondant à une application (512) traitant des contenus dynamiques transmis vers celle-ci,
l'enregistrement d'une application auprès du système de remise de contenus dynamiques génériques par l'enregistrement de l'application auprès du client push possédant une interface d'enregistrement d'applications (514), ledit descriptif d'application contenant des métadonnées de canal,
la mise en mémoire desdites métadonnées de canal dans un entrepôt de métadonnées de canal (570) associé au client push,
la réception d'une enveloppe de métadonnées et de contenus sur le client push par l'intermédiaire d'un proxy push (410), et
le traitement de l'enveloppe de métadonnées et de contenus selon les métadonnées de canal.
- 20
27. Un procédé selon la revendication 26 comprenant en outre :
- l'extraction de métadonnées pour ledit client push de ladite enveloppe de métadonnées et de contenus, et
le traitement de ladite enveloppe de métadonnées et de contenus selon lesdites métadonnées extraites.
- 25
28. Un procédé selon la revendication 27 comprenant en outre le traitement des contenus de ladite enveloppe de métadonnées et de contenus selon lesdites métadonnées extraites.
29. Un procédé selon l'une quelconque des revendications 26 à 28 comprenant en outre l'ordonnancement de la récupération des contenus qui restent à être reçus par le client push (510) par l'intermédiaire dudit proxy push (410).
- 30
30. Un procédé selon la revendication 29 comprenant en outre l'extraction de contenus comme indiqué par un gestionnaire de récupération différée (552) exécutant l'ordonnancement de ladite récupération de contenus.
- 35
31. Un procédé selon la revendication 30 comprenant en outre la mise en mémoire d'un élément parmi les éléments suivants : un contenu, un segment de contenu, une enveloppe de métadonnées et de contenus ou un segment d'enveloppe de métadonnées et de contenus sur le client push (510).
- 40
32. Un procédé selon la revendication 31 comprenant en outre l'une quelconque des opérations suivantes : l'expiration de contenus sensibles au temps conservés en mémoire sur ledit client push (510), le remplacement des contenus conservés en mémoire sur ledit client push par des contenus mis à jour ou la reconstitution de contenus antérieurement divisés en segments en fonction de dépendances de contenus.
- 45
33. Un procédé selon la revendication 26 comprenant en outre l'envoi sélectif de messages de régulation de flux au proxy push (410) de façon à transmettre ladite enveloppe de métadonnées et de contenus au client push (510).
- 50
34. Un procédé selon l'une quelconque des revendications 26, 31 ou 32 comprenant en outre la mise en mémoire de contenus et de métadonnées dans une pluralité de files d'attente de remise (540).
- 55
35. Un procédé selon la revendication 34 comprenant en outre la gestion des contenus et des métadonnées conservés en mémoire dans la pluralité de files d'attente de remise en utilisant au moins un courtier de messages (540).

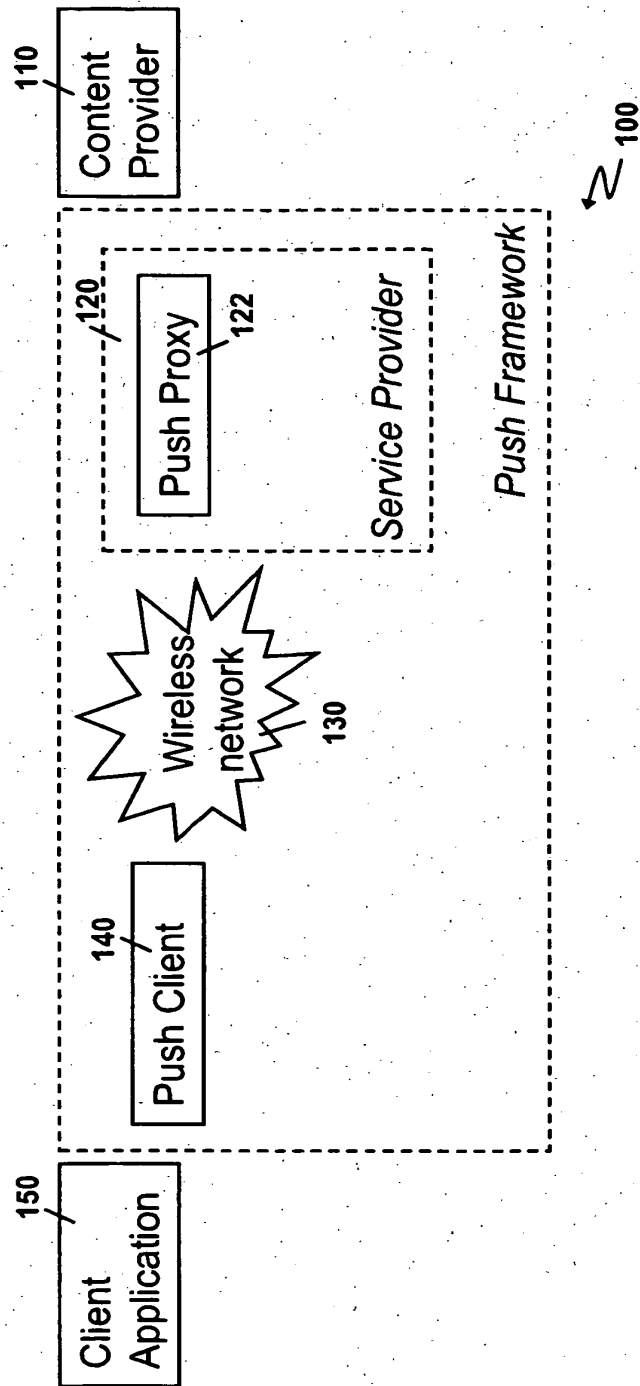


Fig. 1

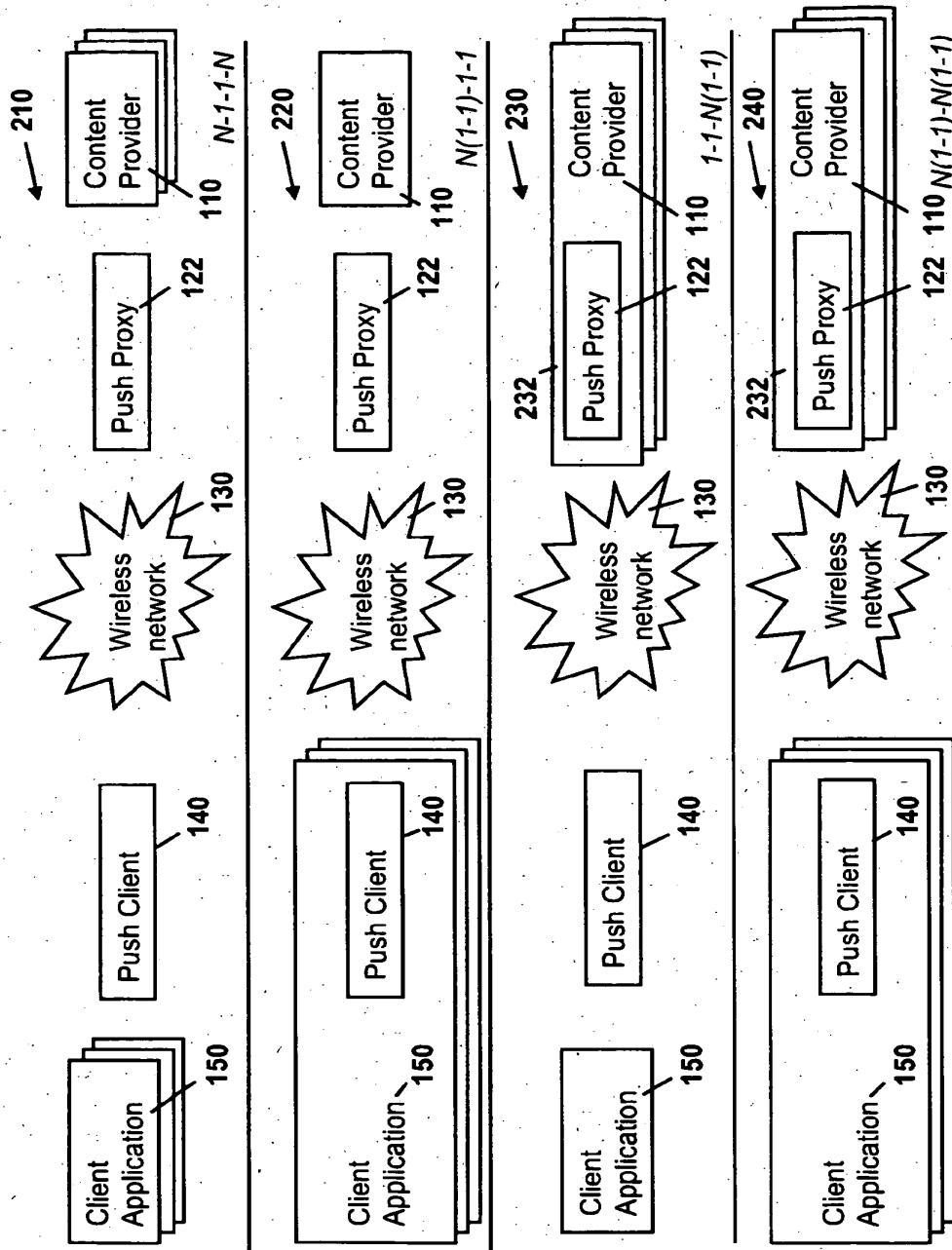


Fig. 2

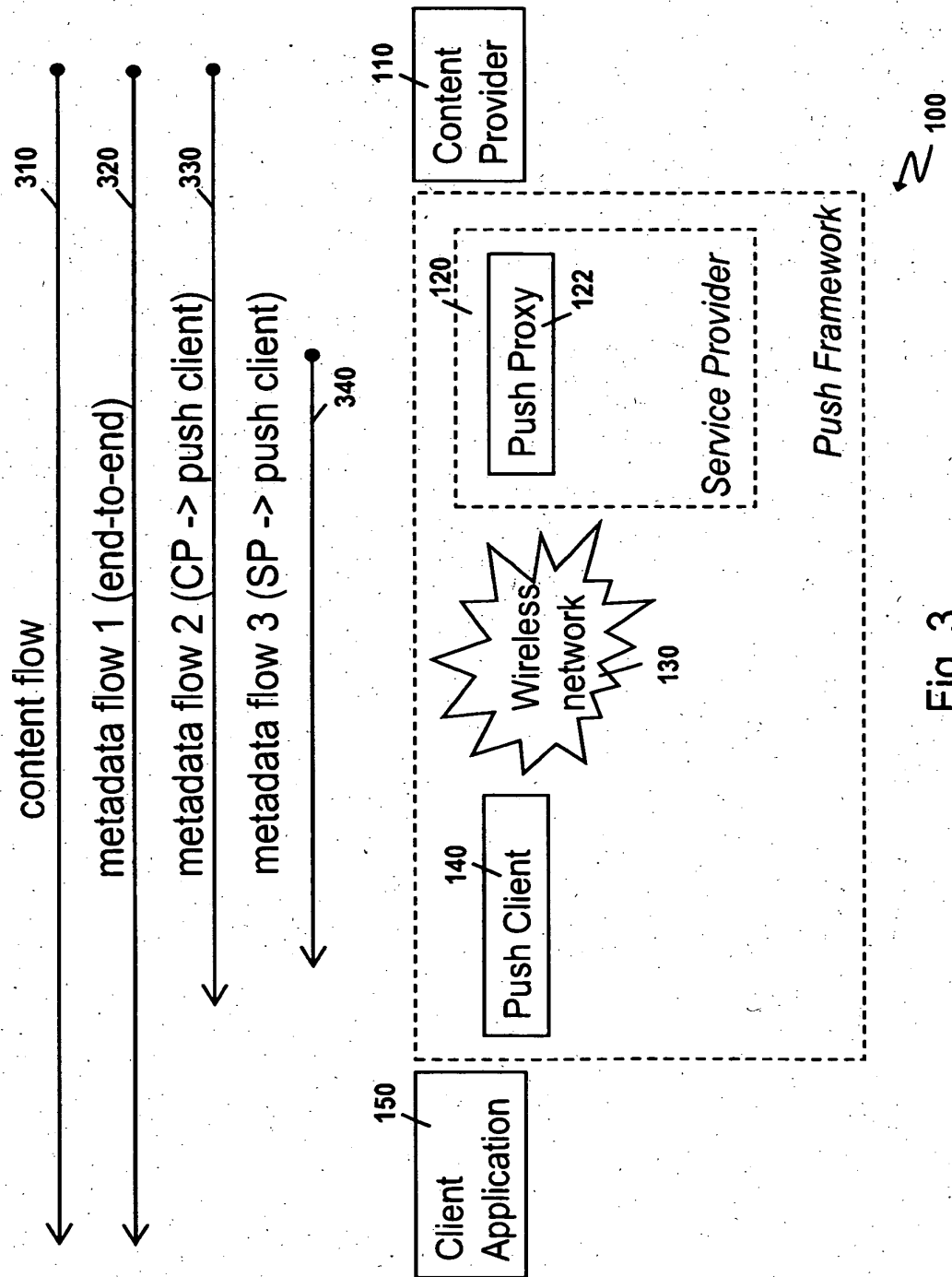


Fig. 3

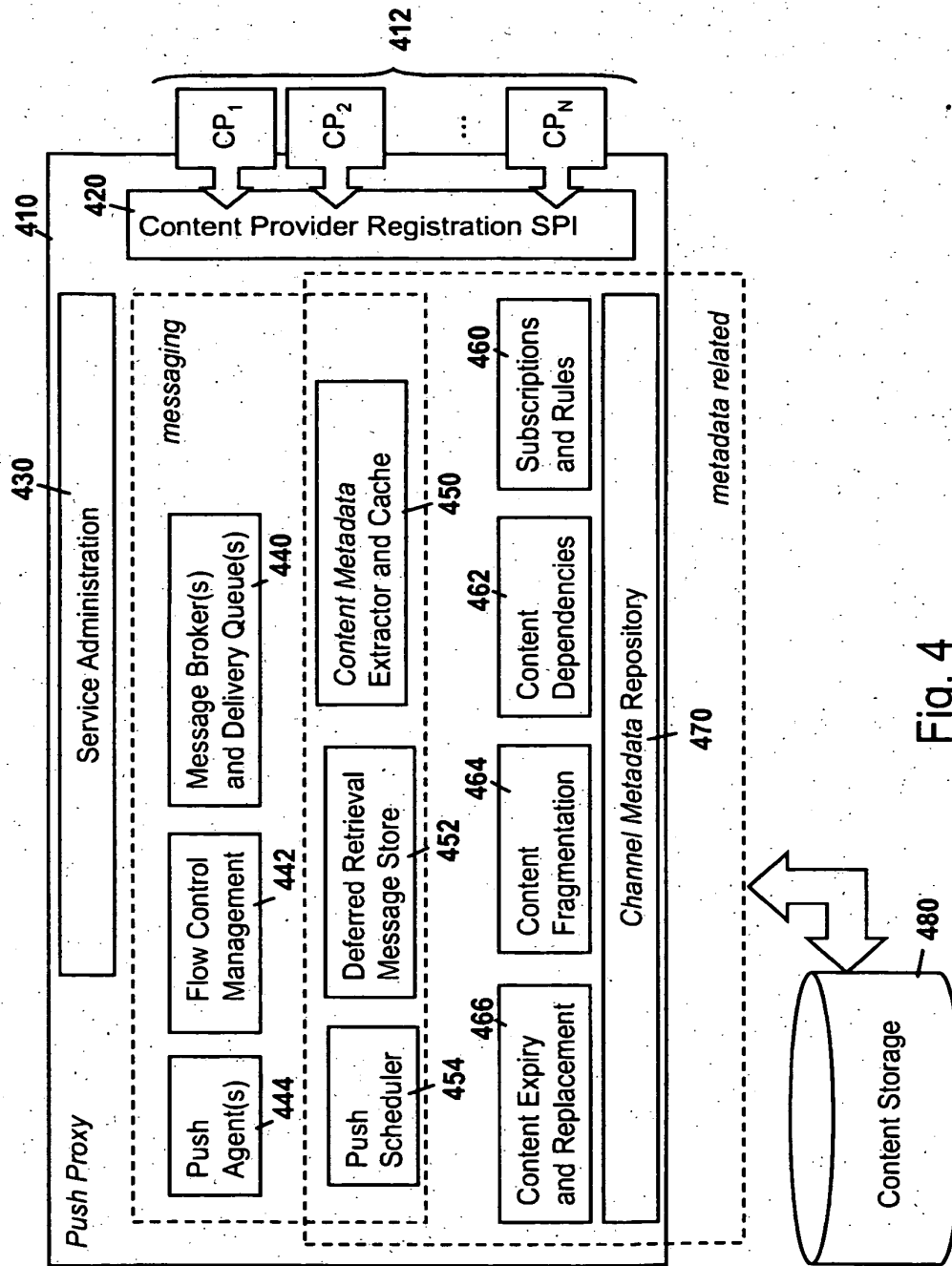


Fig. 4

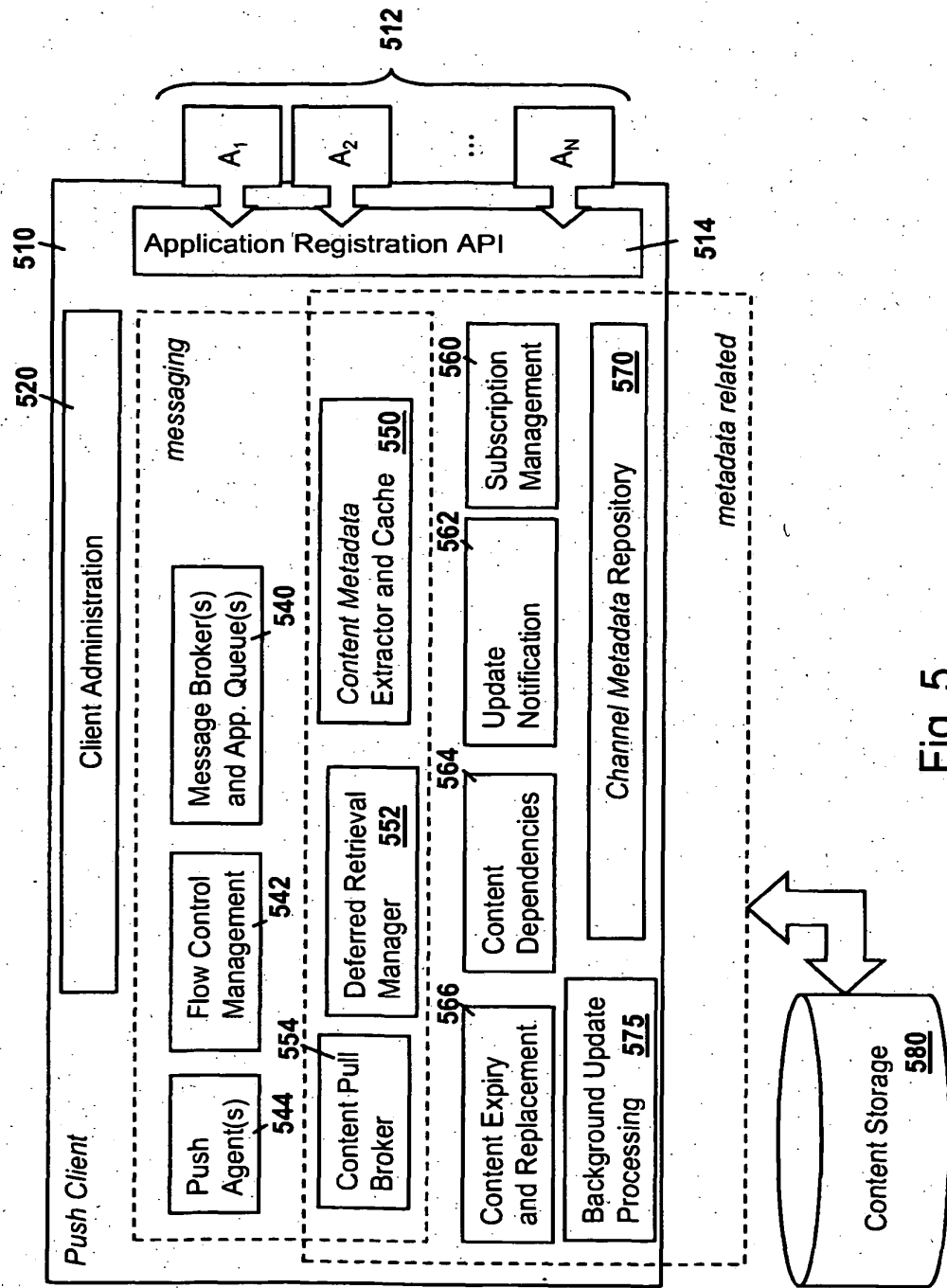


Fig. 5

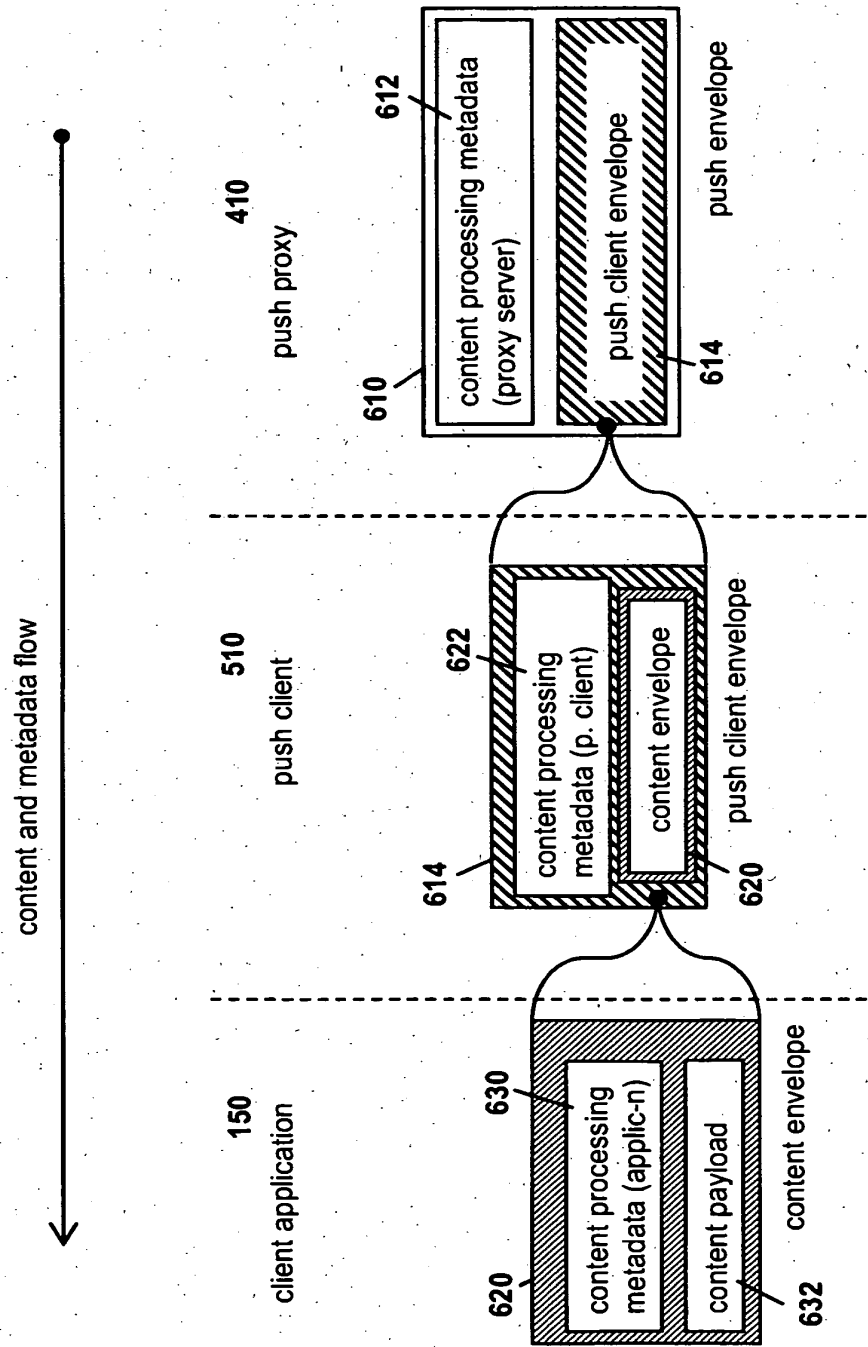


Fig. 6

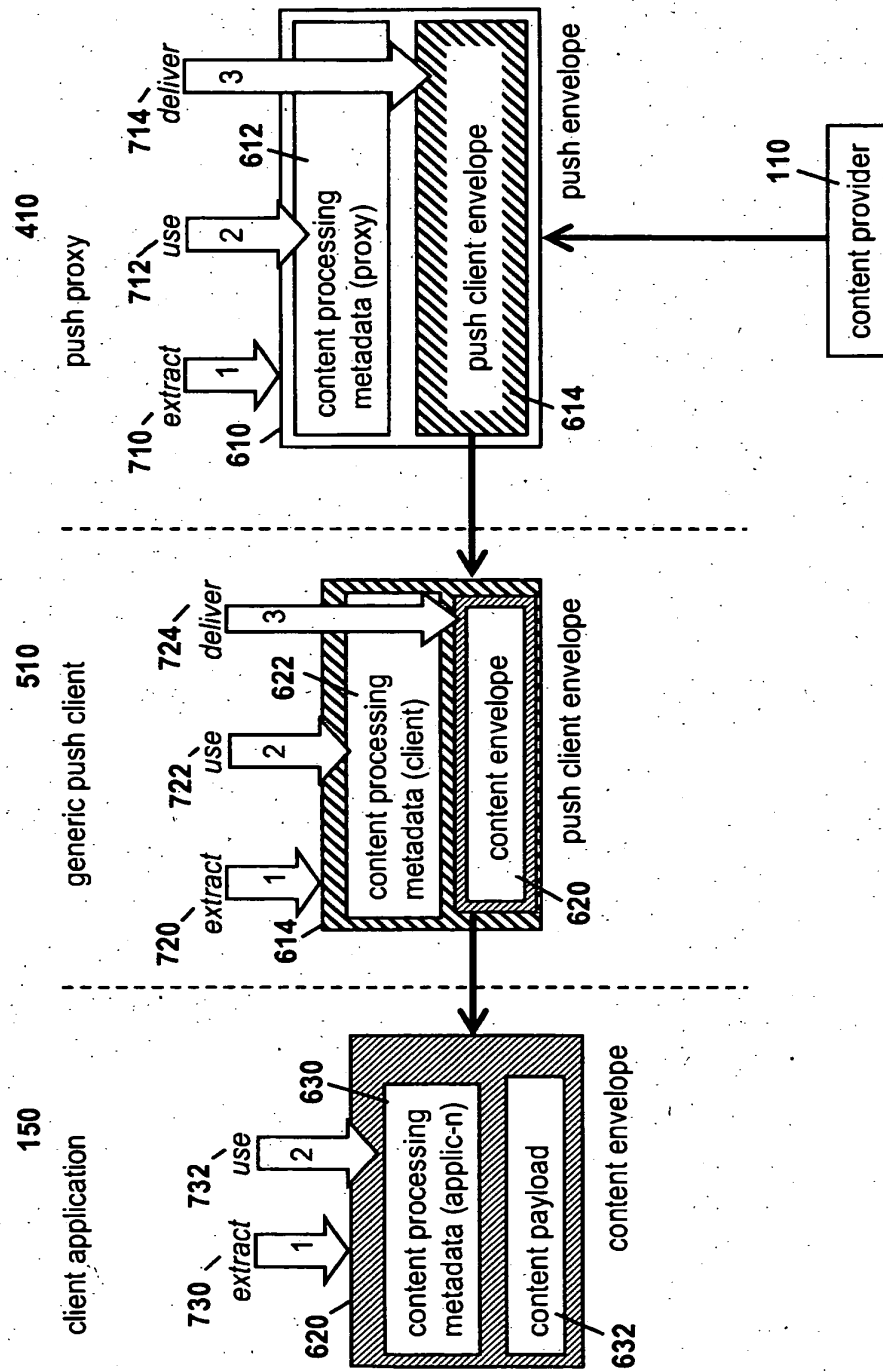


Fig. 7

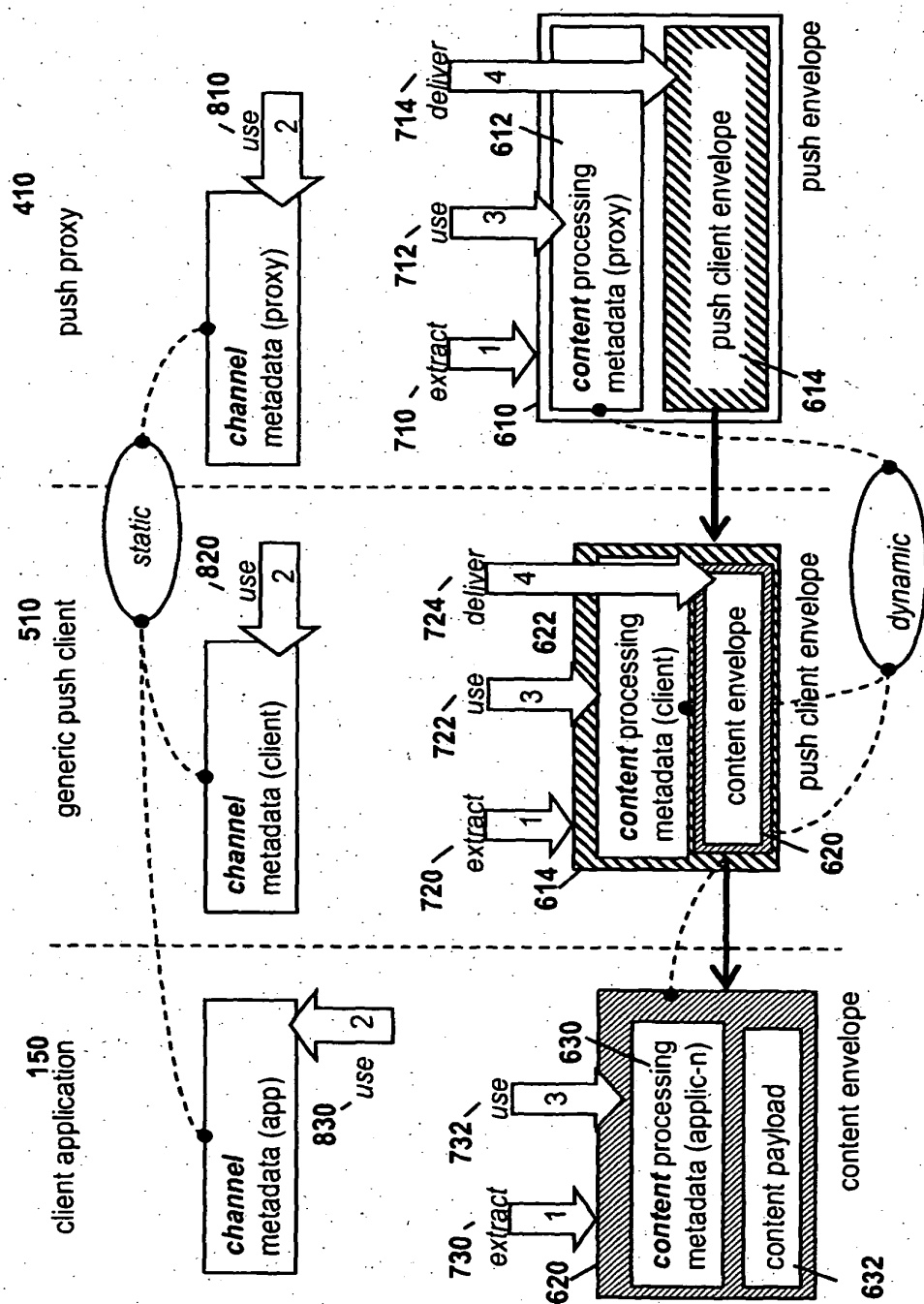
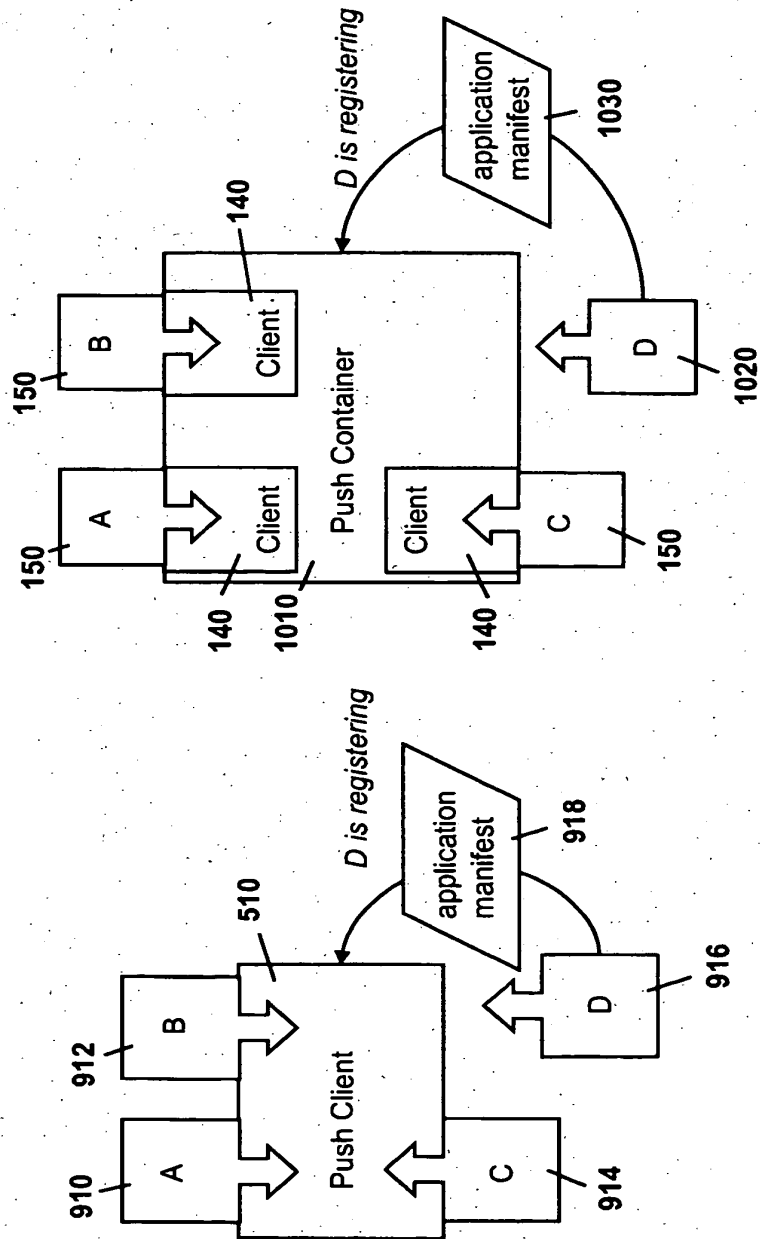
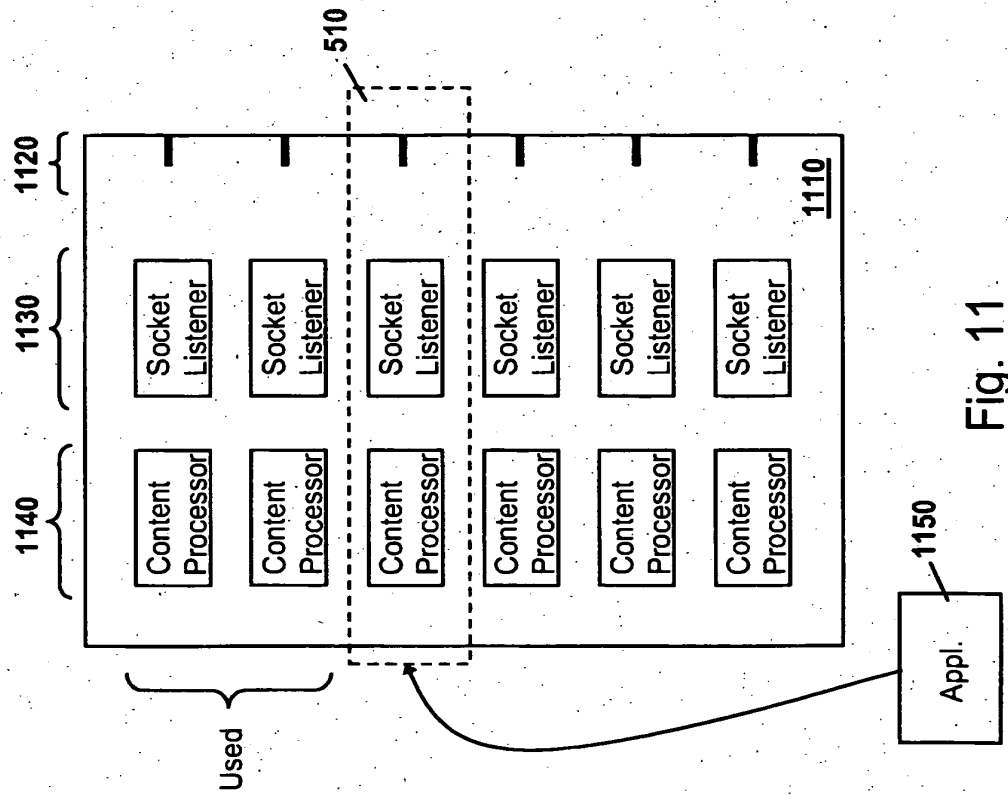


Fig. 8





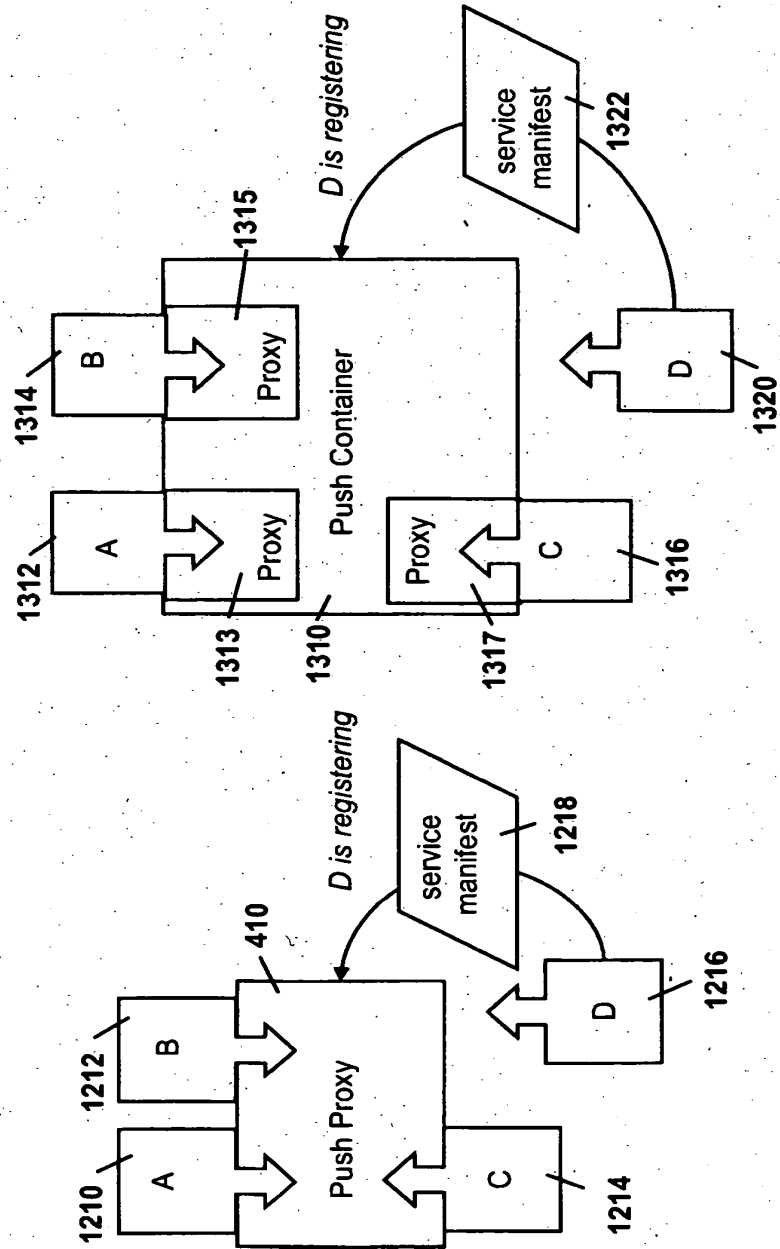


Fig. 13

Fig. 12

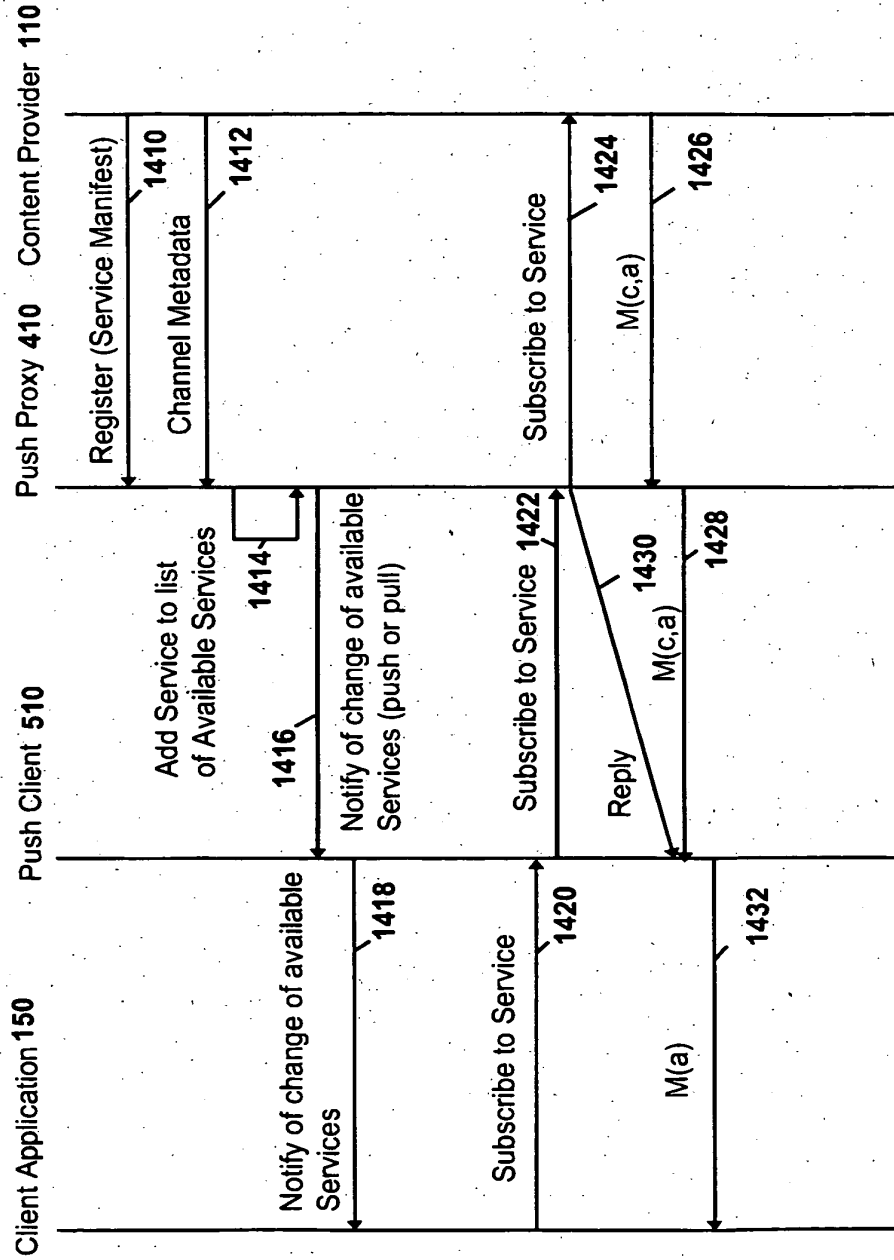


Fig. 14

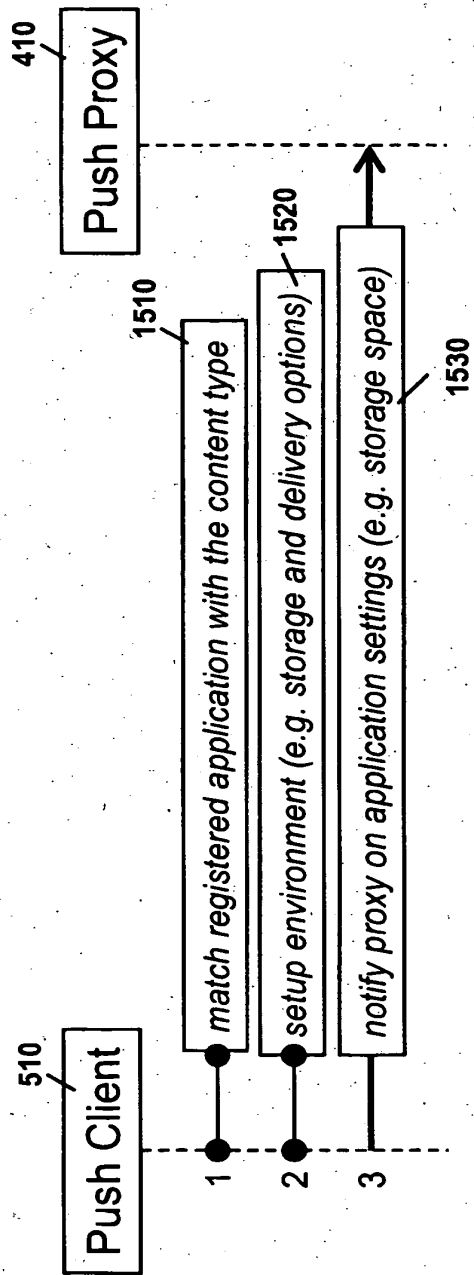


Fig. 15

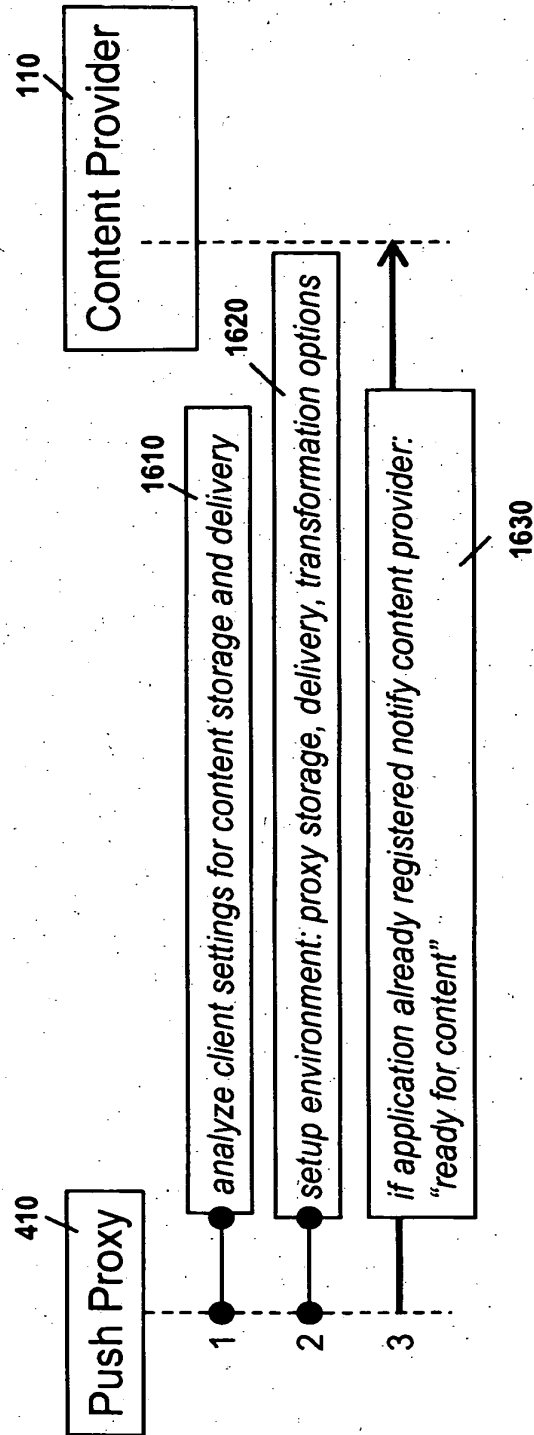


Fig. 16

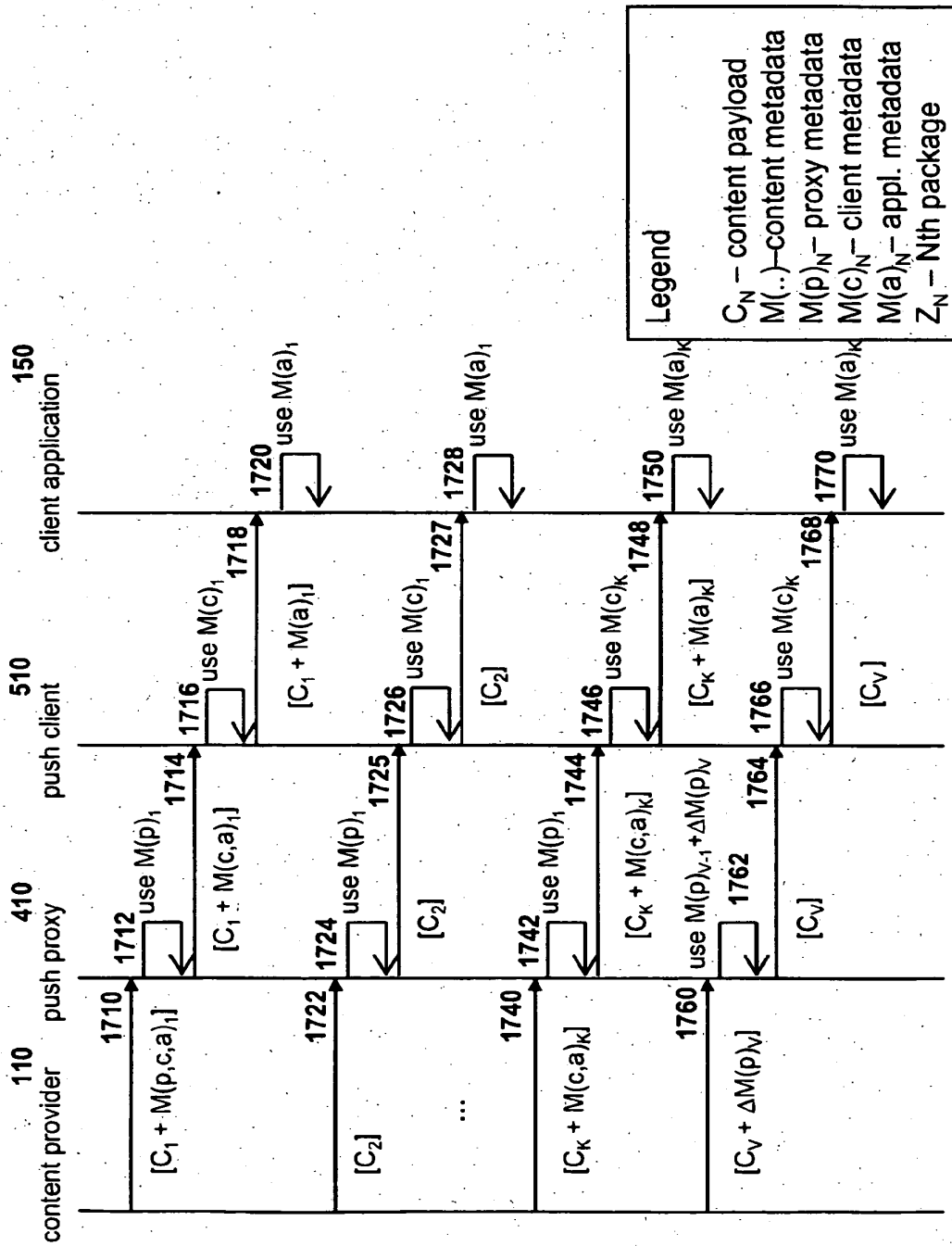


Fig. 17

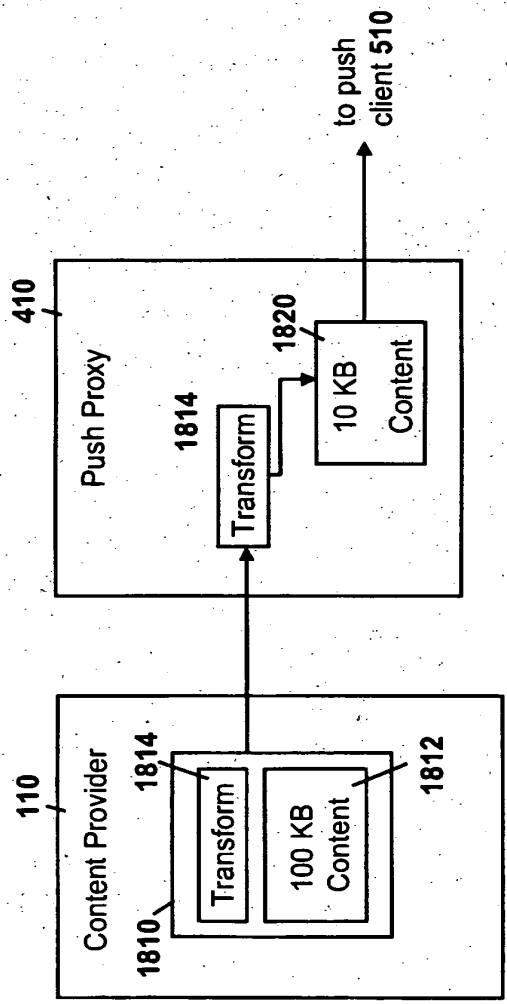


Fig. 18

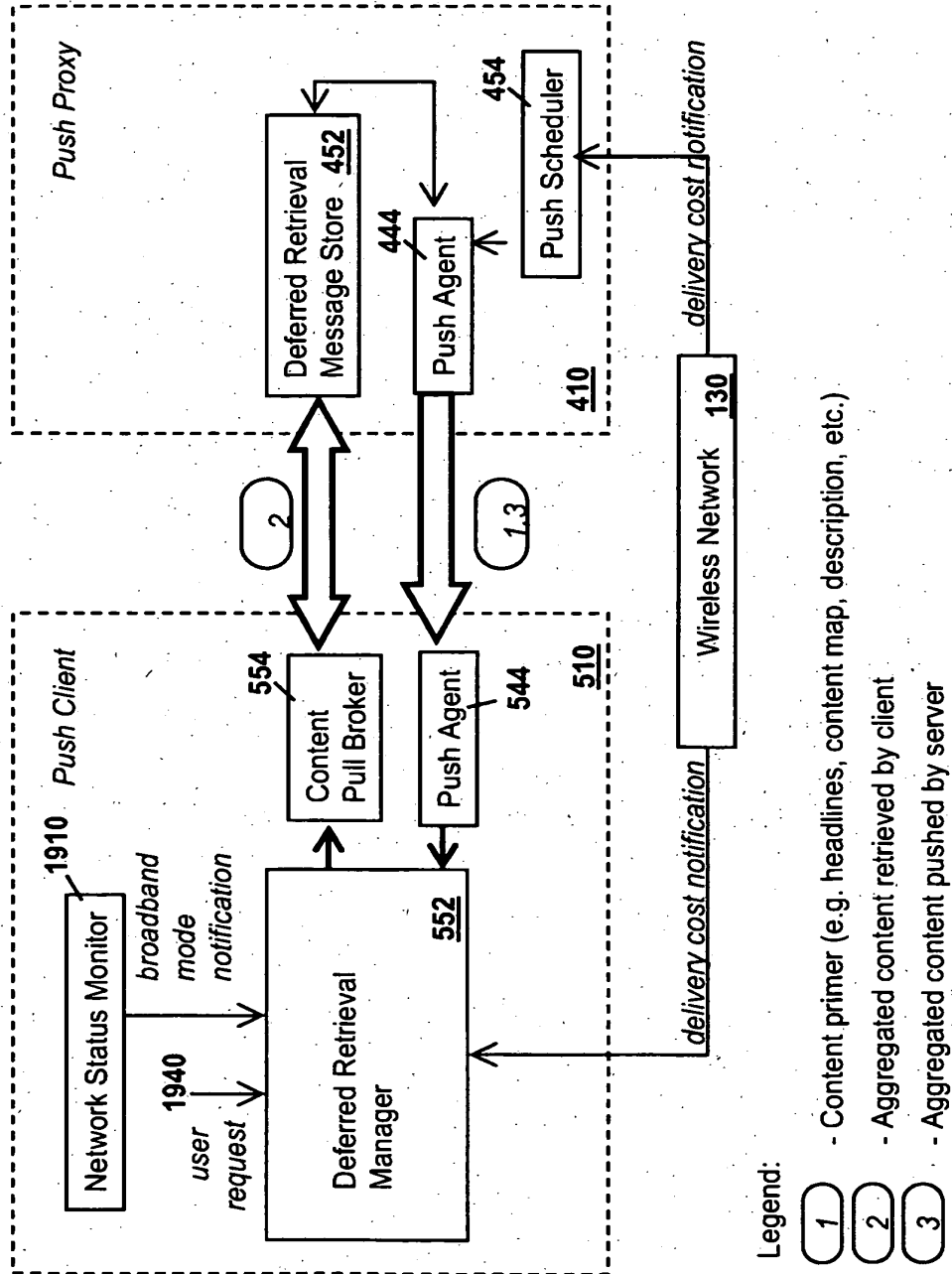


Fig. 19

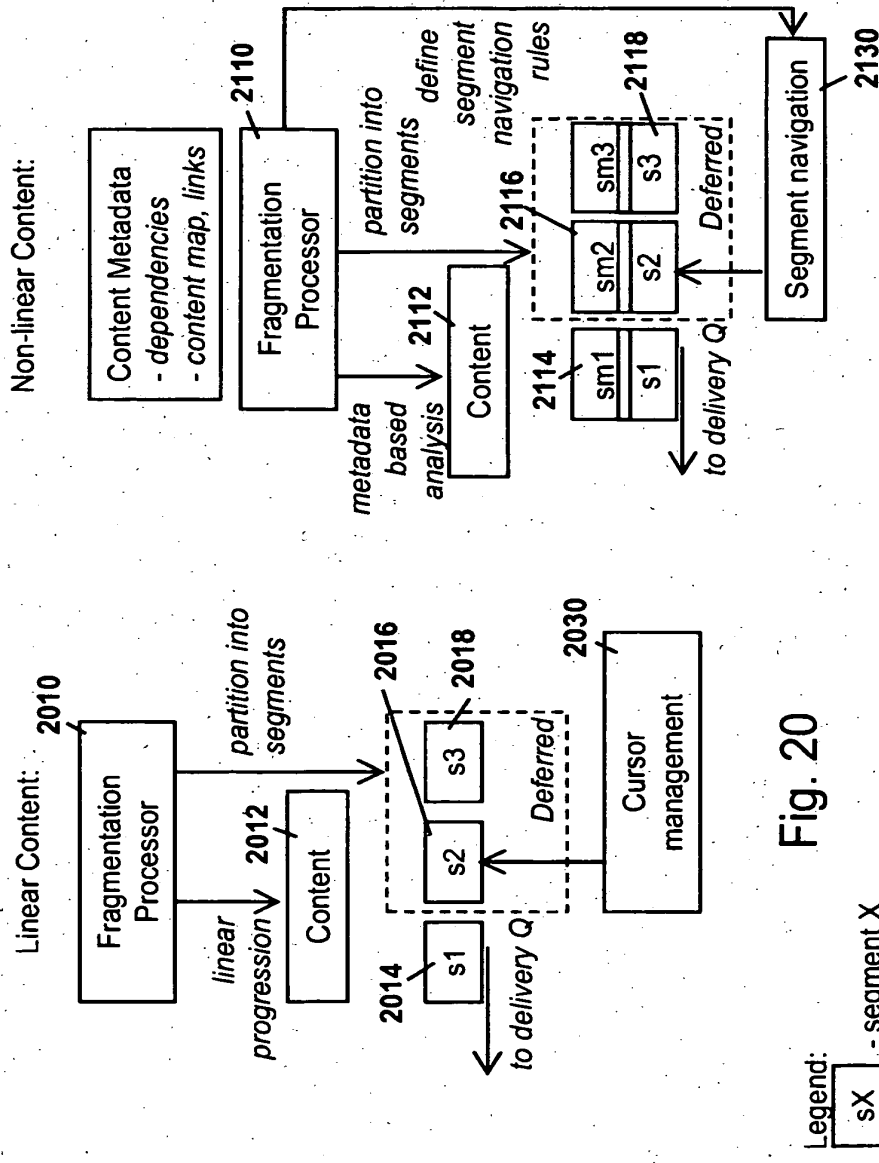


Fig. 20

Fig. 21

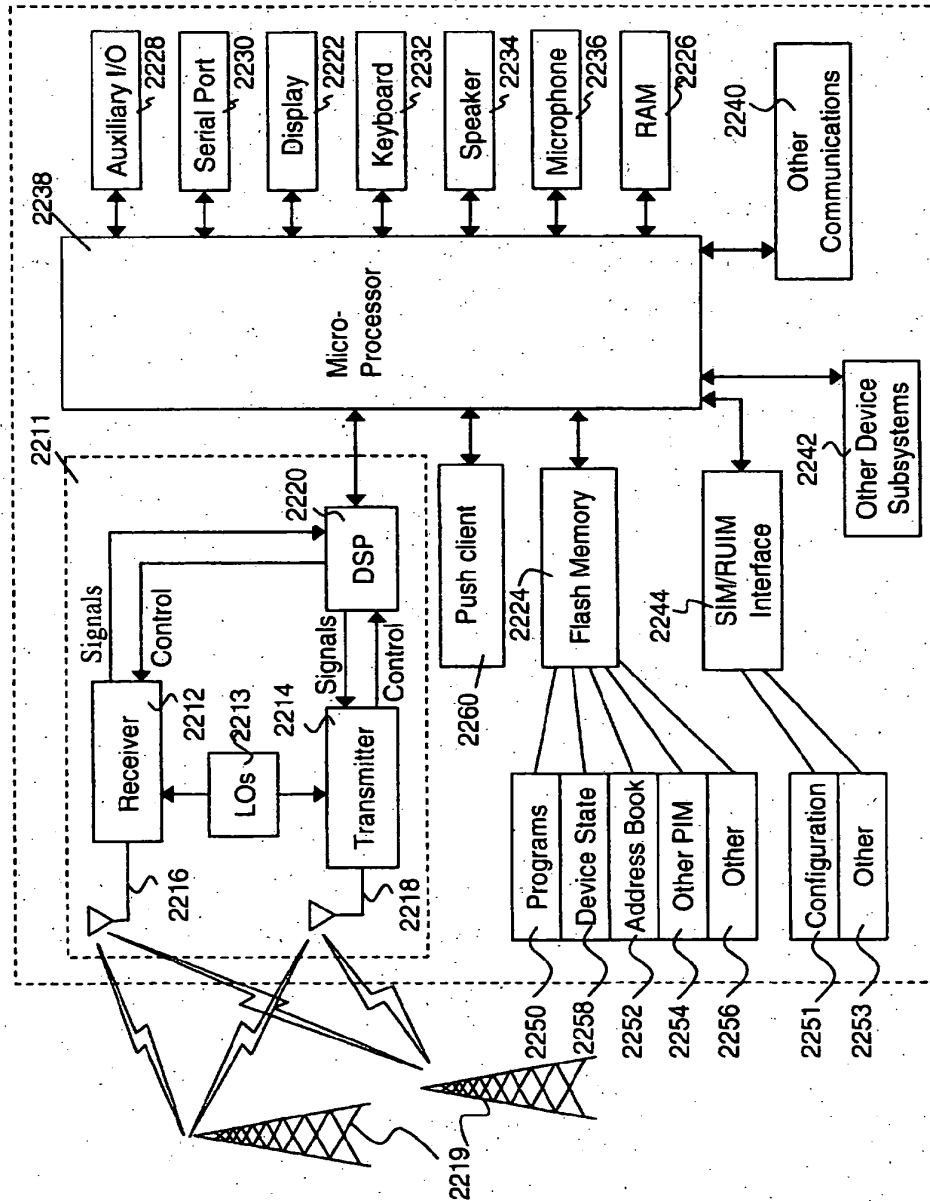


FIG. 22

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	3687		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030229900	A1	2003-12-11	Reisman	
	2	20060135144	A1	2006-06-22	Jothipragasam	
	3	20080082643	A1	2008-04-03	Storrie et al.	
	4	20080124330	A1	2008-05-29	Nakano et al.	
	5	20080134330	A1	2008-06-05	Kapoor et al.	
If you wish to add additional U.S. Published Application citation information please click the Add button.						
FOREIGN PATENT DOCUMENTS						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	3687		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1855817	CN	B	2012-07-04	Mcbride et al.		☐
	2	1247411	EP	A2	2002-10-09	Charas		☐
	3	1247411	EP	B1	2011-11-02	Charas		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	3687
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2023-02-10
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	47518752
Application Number:	17577237
International Application Number:	
Confirmation Number:	5850
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	RALEP007C11C3C2C3C2C1C1C1
Receipt Date:	10-FEB-2023
Filing Date:	17-JAN-2022
Time Stamp:	20:37:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	RALEP007C11C3C2C3C2C1C1C1_1_IDS.pdf	74591 712e7fd755e4767b5960b2fd5cf467d9fea6a2c7	no	4

Warnings:

Information:	
This is not an USPTO supplied IDS fillable form	
Total Files Size (in bytes):	74591
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1

CONFIRMATION NO. 5850

106963
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

PUBLICATION NOTICE



OC000000136176478

Title:Automated Device Provisioning and Activation

Publication No.US-2022-0279021-A1

Publication Date:09/01/2022

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1

CONFIRMATION NO. 5850

POA ACCEPTANCE LETTER

106963
Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691



Date Mailed: 05/26/2022

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/24/2022.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/agizaw/

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 17/577,237		
APPLICATION AS FILED - PART I								
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)	
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	350		N/A		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A		
TOTAL CLAIMS (37 CFR 1.16(j))	1	minus 20 = *	x 50 =	0.00	OR			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1	minus 3 = *	x 240 =	0.00				
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			840				
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00				
				TOTAL		TOTAL		
* If the difference in column 1 is less than zero, enter "0" in column 2.				1670				
APPLICATION AS AMENDED - PART II								
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		OTHER THAN SMALL ENTITY	
	Total (37 CFR 1.16(i))	*	Minus **	x	=	OR	RATE(\$)	
	Independent (37 CFR 1.16(h))	*	Minus ***	x	=	OR	ADDITIONAL FEE(\$)	
	Application Size Fee (37 CFR 1.16(s))					OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR		
				TOTAL ADD'L FEE		TOTAL ADD'L FEE		
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		OTHER THAN SMALL ENTITY	
	Total (37 CFR 1.16(i))	*	Minus **	x	=	OR	RATE(\$)	
	Independent (37 CFR 1.16(h))	*	Minus ***	x	=	OR	ADDITIONAL FEE(\$)	
	Application Size Fee (37 CFR 1.16(s))					OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR		
				TOTAL ADD'L FEE		TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.								



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
17/577,237	01/17/2022	2414	1750	RALEP007C11C3C2C3C2C1C1C1	1	1

CONFIRMATION NO. 5850

UPDATED FILING RECEIPT



0000000134093098

106963

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

Date Mailed: 05/26/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Gregory G. Raleigh, Incline Village, NV;

Applicant(s)

Headwater Research LLC, Tyler, TX;

Assignment For Published Patent Application

Headwater Research LLC, Tyler, TX

Power of Attorney: The patent practitioners associated with Customer Number 106963

Domestic Priority data as claimed by applicant

This application is a CON of 16/436,628 06/10/2019 PAT 11228617
which is a CON of 15/582,350 04/28/2017 PAT 10321320
which is a CON of 15/239,398 08/17/2016 PAT 9641957
which is a CON of 14/979,233 12/22/2015 PAT 9532161
which is a CON of 14/667,353 03/24/2015 PAT 9232403
which is a CON of 14/263,604 04/28/2014 PAT 9037127
which is a CON of 12/380,780 03/02/2009 PAT 8839388
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 01/25/2022

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/577,237**

Projected Publication Date: 09/01/2022

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Automated Device Provisioning and Activation

Preliminary Class

370

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign

page 2 of 4

patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1

CONFIRMATION NO. 5850

FORMALITIES LETTER

106963
Headwater Research LLC
110 North College Avenue
Suite 1116
Tyler, TX 75702



Date Mailed: 01/27/2022

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.

The surcharge is due for any one of:

- late submission of the basic filing fee, search fee, or examination fee,
- late submission of inventor's oath or declaration,
- filing an application that does not contain at least one claim on filing, or
- submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- \$ **80** basic filing fee.
- \$ **840** for **160** electronically equivalent pages in excess of **100** application size fee.
- \$ **80** surcharge.
- \$ **350** search fee.
- \$ **400** examination fee.
- \$(**0**) previous unapplied payment amount.
- \$ **1750** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice".
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/elbanaybanay/

Electronic Patent Application Fee Transmittal				
Application Number:		17577237		
Filing Date:		17-Jan-2022		
Title of Invention:		Automated Device Provisioning and Activation		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		Michael Farjami/Evan Gunderman		
Attorney Docket Number:		RALEP007C11C3C2C3C2C1C1C1		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
Pages:				
UTILITY APPL SIZE FEE PER 50 SHEETS >100	2081	4	210	840
Claims:				
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	2051	1	80	80

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	2252	1	320	320
Miscellaneous:				
Total in USD (\$)				2070

Electronic Acknowledgement Receipt	
EFS ID:	45791535
Application Number:	17577237
International Application Number:	
Confirmation Number:	5850
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	RALEP007C11C3C2C3C2C1C1C1
Receipt Date:	24-MAY-2022
Filing Date:	17-JAN-2022
Time Stamp:	15:25:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$2070
RAM confirmation Number	E20225NF28244902
Deposit Account	500731
Authorized User	Evan Gunderman
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		RALEP007C11C3C2C3C2C1C1C1_Resp_to_Notice_to_File_Missing_Parts_May_24_22.pdf	236895	yes	5
			e820cce36feb88a2eb50f2b4b74bcd3347238c6		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	2	
	Extension of Time		3	3	
	Miscellaneous Incoming Letter		4	5	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	51022	no	2
			a14c7da0399adbdbd770f1ffe9249b2cd787b4f		
Warnings:					
Information:					
Total Files Size (in bytes):			287917		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: May 24, 2022

To: United States Patent and Trademark Office
Examiner: Unknown; Art Unit: 2414

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 5

Message:

Enclosed, please find:

1. Response to Notice to File Missing Parts of Non-Provisional Application;
2. Copy of Notice to File Missing Parts, dated January 27, 2022

Credit card payment in the amount of **\$2,070.00** as the required Filing fee, Excess pages fee, surcharge, search fee, examination fee and two month extension fee is hereby included with this filing

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account No. **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh	Group Art Unit: 2424
Application Serial No.: 17/577,237	Examiner: Unknown
Filed: 1/17/2022	
Title: Automated Device Provisioning and Activation	

**RESPONSE TO NOTICE TO FILE MISSING PARTS
OF NONPROVISIONAL APPLICATION**

Mail Stop Missing Parts
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

In response to the Notice to File Missing Parts, dated January 27, 2022, in the above-captioned application, enclosed please find the required filing fees. Applicant respectfully requests a two-month extension for filing the present response.

The USPTO is hereby authorized to charge our Deposit Account Number **50-0731** for any deficiencies or to credit our account for any overpayments.

Respectfully submitted,
Farjami & Farjami LLP

By: /Farshad Farjami/
Farshad Farjami, Esq.
Reg. No. 41,014

Farshad Farjami
FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Ste. 360
Mission Viejo, CA 92691
Tel: (949) 282-1000
Fax: (949) 282-1002

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.

May 24, 2022
Date

Evan C. Gunderman
Name

/evan c. gunderman/
Signature

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) P007C11C3C2C3C2C1C1C1																														
Application Number 17/577,237	Filed 01/17/2020																															
For Automated Device Provisioning and Activation																																
Art Unit 2414	Examiner not assigned																															
<p>This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.</p> <p>The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;"></th> <th style="width: 15%; text-align: center;"><u>Fee</u></th> <th style="width: 15%; text-align: center;"><u>Small Entity Fee</u></th> <th style="width: 15%; text-align: center;"><u>Micro Entity Fee</u></th> <th style="width: 15%;"></th> </tr> </thead> <tbody> <tr> <td>☐ One month (37 CFR 1.17(a)(1))</td> <td style="text-align: center;">\$220</td> <td style="text-align: center;">\$110</td> <td style="text-align: center;">\$55</td> <td style="text-align: right;">\$ _____</td> </tr> <tr> <td>☒ Two months (37 CFR 1.17(a)(2))</td> <td style="text-align: center;">\$640</td> <td style="text-align: center;">\$320</td> <td style="text-align: center;">\$160</td> <td style="text-align: right;">\$ 320</td> </tr> <tr> <td>☐ Three months (37 CFR 1.17(a)(3))</td> <td style="text-align: center;">\$1,480</td> <td style="text-align: center;">\$740</td> <td style="text-align: center;">\$370</td> <td style="text-align: right;">\$ _____</td> </tr> <tr> <td>☐ Four months (37 CFR 1.17(a)(4))</td> <td style="text-align: center;">\$2,320</td> <td style="text-align: center;">\$1,160</td> <td style="text-align: center;">\$580</td> <td style="text-align: right;">\$ _____</td> </tr> <tr> <td>☐ Five months (37 CFR 1.17(a)(5))</td> <td style="text-align: center;">\$3,160</td> <td style="text-align: center;">\$1,580</td> <td style="text-align: center;">\$790</td> <td style="text-align: right;">\$ _____</td> </tr> </tbody> </table> <p>☐ Applicant asserts small entity status. See 37 CFR 1.27.</p> <p>☐ Applicant certifies micro entity status. See 37 CFR 1.29. Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.</p> <p>☐ A check in the amount of the fee is enclosed.</p> <p>☐ Payment by credit card. Form PTO-2038 is attached.</p> <p>☐ The Director has already been authorized to charge fees in this application to a Deposit Account.</p> <p>☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number <u>50-0731</u>.</p> <p>☐ Payment made via EFS-Web.</p> <p>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</p> <p>I am the</p> <p>☐ applicant/inventor.</p> <p>☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).</p> <p>☒ attorney or agent of record. Registration number <u>41,014</u></p> <p>☐ attorney or agent acting under 37 CFR 1.34. Registration number _____</p> <p><u>/FARSHAD FARJAMI/</u> <u>May 24, 2022</u></p> <p style="text-align: center;">Signature Date</p> <p><u>FARSHAD FARJAMI</u> <u>(949) 282-1000</u></p> <p style="text-align: center;">Typed or printed name Telephone Number</p> <p>NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.</p> <p>☐ * Total of _____ forms are submitted.</p>				<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>		☐ One month (37 CFR 1.17(a)(1))	\$220	\$110	\$55	\$ _____	☒ Two months (37 CFR 1.17(a)(2))	\$640	\$320	\$160	\$ 320	☐ Three months (37 CFR 1.17(a)(3))	\$1,480	\$740	\$370	\$ _____	☐ Four months (37 CFR 1.17(a)(4))	\$2,320	\$1,160	\$580	\$ _____	☐ Five months (37 CFR 1.17(a)(5))	\$3,160	\$1,580	\$790	\$ _____
	<u>Fee</u>	<u>Small Entity Fee</u>	<u>Micro Entity Fee</u>																													
☐ One month (37 CFR 1.17(a)(1))	\$220	\$110	\$55	\$ _____																												
☒ Two months (37 CFR 1.17(a)(2))	\$640	\$320	\$160	\$ 320																												
☐ Three months (37 CFR 1.17(a)(3))	\$1,480	\$740	\$370	\$ _____																												
☐ Four months (37 CFR 1.17(a)(4))	\$2,320	\$1,160	\$580	\$ _____																												
☐ Five months (37 CFR 1.17(a)(5))	\$3,160	\$1,580	\$790	\$ _____																												

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	45791192
Application Number:	17577237
International Application Number:	
Confirmation Number:	5850
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	RALEP007C11C3C2C3C2C1C1C1
Receipt Date:	24-MAY-2022
Filing Date:	17-JAN-2022
Time Stamp:	15:08:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		RALEP007C11C3C2C3C2C1C1C1_1_POA_May_24_22.pdf	230722	yes	4
			6a78bc4b1a6e2f1520ce7e21790e8b836fe3e08f		

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Transmittal Letter	1	1
	Power of Attorney	2	4
Warnings:			
Information:			
Total Files Size (in bytes):		230722	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>			



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: May 24, 2022

To: United States Patent and Trademark Office
Examiner: Unknown; Art Unit: 2424

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 4

Message:

Enclosed, please find:

1. Transmittal for Power of Attorney (Form PTO/AIA/96); and
2. Power of Attorney Document (Form PTO/SB/80).

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

Thank you.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Headwater Research LLC
Application No./Patent No.: 17/577,237 Filed/Issue Date: 01/17/2022
Titled: Automated Device Provisioning and Activation
Headwater Research LLC, a limited liability company
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
- B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Inventor (Raleigh) To: Headwater Partners I LLC

The document was recorded in the United States Patent and Trademark Office at
Reel 059199, Frame 0148, or for which a copy thereof is attached.

2. From: Headwater Partners I LLC To: Headwater Research LLC

The document was recorded in the United States Patent and Trademark Office at
Reel 059199, Frame 0214, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Farshad Farjami/

May 24, 2022

Signature

Date

Farshad Farjami

41,014

Printed or Typed Name

Title or Registration Number

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:



Practitioners associated with the Customer Number:

106963

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:



The address associated with Customer Number:

106963

OR

☐ Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

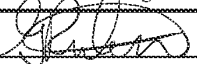
Assignee Name and Address:

Headwater Research LLC
110 North College Avenue, Suite 1116
Tyler, TX 75702

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	May 20, 2022
Name	Gregory G. Raleigh	Telephone	(650) 740-4781
Title	Lead Director, Headwater Research LLC		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh, Gregory	Examiner: NOT YET ASSIGNED
Serial No.: 17/577,237	Art Unit: 2414
Filed: January 17, 2022	Conf. No.: 5850
Title: Automated Device Provisioning and Activation	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

The references cited on attached form PTO/SB/08A are being called to the attention of the Examiner. Copies of the references are not enclosed.

In accordance with 37 CFR §1.98(d), copies of the references can be found in related U.S. Patent Application No. 16/436,628 filed June 10, 2019, of which the instant application is a continuation, or in related U.S. Patent Application No. 15/582,350 filed on April 28, 2017, of which 16/436,628 is a continuation.

It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the “references cited” on any patent to issue therefrom.

As provided for by 37 CFR § 1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement, but if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. **50-0731**.

Respectfully submitted,
Farjami & Farjami LLP

Date: May 23, 2022

By: /Farshad Farjami/
Farshad Farjami, Esq.
Reg. No. 41,014

FARJAMI & FARJAMI LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691
Tel: (949) 282-1000
Fax: (949) 282-1002

<u>CERTIFICATE OF ELECTRONIC TRANSMISSION</u>	
I hereby certify that this correspondence is being filed via EFS in United States Patent and Trademark Office, on the date stated below.	
<u>May 24, 2022</u>	
Date	
<u>Evan C. Gunderman</u>	<u>/evan c. gunderman /</u>
Name	Signature

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	10027819	B2	2018-07-17	Lu et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20010048738	A	2001-12-06	Baniak, Paul G. et al.	
	2	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	3	20020013844	A1	2002-01-31	Garrett et al.	
	4	20020022472		2002-02-21	WATLER et al.	
	5	20020022483	A1	2002-02-21	Thompson et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

6	20020049074	A	2002-04-25	Eisinger, Bernd et al.	
7	20020099848	A1	2002-07-25	Lee, Hoon	
8	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	
9	20020120370	A1	2002-08-29	Parupudi et al.	
10	20020120540		2002-08-29	KENDE et al.	
11	20020131404		2002-09-19	MEHTA et al.	
12	20020138599	A1	2002-09-26	Dilman et al.	
13	20020138601		2002-09-26	PIPONIUS et al.	
14	20020154751	A1	2002-10-24	Thompson et al.	
15	20020161601	A	2002-10-31	Nauer, Bernhard et al.	
16	20020164983		2002-11-07	Raviv, Li-On et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

17	20020176377		2002-11-28	HAMILTON, Thomas E.	
18	20020188732	A1	2002-12-12	Buckman et al.	
19	20020191573	A1	2002-12-19	Whitehill et al.	
20	20020199001		2002-12-26	WENOCUR et al.	
21	20030004937		2003-01-02	SALMENKAITA et al.	
22	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
23	20030013434		2003-01-16	ROSENBERG et al.	
24	20030018524		2003-01-23	FISHMAN et al.	
25	20030028623	A1	2003-02-06	Hennessey et al.	
26	20030046396		2003-03-06	RICHTER et al.	
27	20030050070		2003-03-13	MASHINSKY et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	28	20030050837		2003-03-13	KIM, Do Sik	
	29	20030084321	A1	2003-05-01	Tarquini et al.	
	30	20030088671	A1	2003-05-08	Klinker et al.	
	31	20030133408		2003-07-17	CHENG et al.	
	32	20030134650	A1	2003-07-17	Sundar et al.	
	33	20030159030	A1	2003-08-21	Evans, Junius A.	
	34	20030161265		2003-08-28	CAO et al.	
	35	20030171112		2003-09-11	Lupper, Alfred et al.	
	36	20030182420		2003-09-25	JONES et al.	
	37	20030182435		2003-09-25	REDLICH et al.	
	38	20030184793	A1	2003-10-02	Pineau, Richard A.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

39	20030188006	A	2003-10-02	Bard, Steven R.	
40	20030188117	A	2003-10-02	Yoshino et al.	
41	20030220984		2003-11-27	JONES et al.	
42	20030224781		2003-12-04	MILFORD et al.	
43	20030229900		2003-12-11	REISMAN, Richard	
44	20030233332	A	2003-12-18	Keeler, James D. et al.	
45	20030236745		2003-12-25	HARTSELL et al.	
46	20040019539		2004-01-29	RAMAN et al.	
47	20040019564	A1	2004-01-29	Goldthwaite et al.	
48	20040021697		2004-02-05	BEATON et al.	
49	20040024756	A1	2004-02-05	Rickard, John Terrell	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

50	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
51	20040039792	A1	2004-02-26	Nakanishi, Tornoaki	
52	20040044623		2004-03-04	WAKE et al.	
53	20040047358		2004-03-11	CHEN et al.	
54	20040054779	A1	2004-03-18	Takeshima et al.	
55	20040073672		2004-04-15	FASCENDA, Anthony C.	
56	20040082346		2004-04-29	SKYTT et al.	
57	20040098715		2004-05-20	AGHERA et al.	
58	20040102182	A	2004-05-27	Reith, Lothar et al.	
59	20040103193		2004-05-27	PANDYA et al.	
60	20040107360		2004-06-03	HERRMANN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	61	20040116140	A1	2004-06-17	Babbar et al.	
	62	20040127200		2004-07-01	SHAW et al.	
	63	20040127208	A1	2004-07-01	Nair et al.	
	64	20040127256	A1	2004-07-01	Goldthwaite et al.	
	65	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	66	20040133668	A1	2004-07-08	Nicholas III, Henry T.	
	67	20040137890	A1	2004-07-15	Kaike, Catherine	
	68	20040165596	A1	2004-08-26	Garcia et al.	
	69	20040167958	A1	2004-08-26	Stewart et al.	
	70	20040168052		2004-08-26	CLISHAM et al.	
	71	20040170191	A	2004-09-02	Guo et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

72	20040176104	A1	2004-09-09	Arcens	
73	20040198331		2004-10-07	COWARD et al.	
74	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
75	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
76	20040225561	A1	2004-11-11	Hertzberg et al.	
77	20040225898	A	2004-11-11	Frost, D. et al.	
78	20040236547		2004-11-25	RAPPAPORT et al.	
79	20040243680	A1	2004-12-02	Mayer, Georg	
80	20040243992	A	2004-12-02	Gustafson et al.	
81	20040249918		2004-12-09	SUNSHINE, Roger N.	
82	20040255145	A	2004-12-16	Chow, Jerry	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

83	20040259534	A1	2004-12-23	Chaudhari et al.	
84	20040260766	A1	2004-12-23	Barros et al.	
85	20040267872	A1	2004-12-30	Serdy et al.	
86	20050007993		2005-01-13	Chambers, Mahdi et al.	
87	20050009499		2005-01-13	KOSTER, Karl	
88	20050021995		2005-01-27	LAL et al.	
89	20050041617	A1	2005-02-24	Huotari et al.	
90	20050048950		2005-03-03	MORPER, Hans-Jochen	
91	20050055291		2005-03-10	BEVENTE et al.	
92	20050055309		2005-03-10	WILLIAMS et al.	
93	20050055595	A	2005-03-10	Frazer et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

94	20050060266		2005-03-17	DEMELLO et al.	
95	20050060525	A1	2005-03-17	Schwartz et al.	
96	20050075115	A1	2005-04-07	Cornelle et al.	
97	20050079863	A	2005-04-14	Macaluso, Anthony G.	
98	20050091505	A1	2005-04-28	Riley et al.	
99	20050096024	A1	2005-05-05	Bicker et al.	
100	20050097516		2005-05-05	DONNELLY et al.	
101	20050107091		2005-05-19	VANNITHAMBY et al.	
102	20050108075	A1	2005-05-19	Douglas et al.	
103	20050111463	A1	2005-05-26	Leung et al.	
104	20050128967		2005-06-16	SCOBIE, Donald MacGregor	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	105	20050135264	A1	2005-06-23	Popoff et al.	
	106	20050163320	A1	2005-07-28	Brown et al.	
	107	20050166043		2005-07-28	ZHANG et al.	
	108	20050183143		2005-08-18	ANDERHOLM et al.	
	109	20050186948	A	2005-08-25	Gallagher et al.	
	110	20050198377		2005-09-08	FERGUSON et al.	
	111	20050216421		2005-09-29	BARRY et al.	
	112	20050228985		2005-10-13	YLIKOSKI et al.	
	113	20050238046		2005-10-27	HASSAN et al.	
	114	20050239447	A1	2005-10-27	Holzman et al.	
	115	20050245241	A1	2005-11-03	Durand et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

116	20050246282		2005-11-03	NASLUND et al.	
117	20050250508		2005-11-10	GUO et al.	
118	20050250536	A1	2005-11-10	Deng et al.	
119	20050254435		2005-11-17	MOAKLEY et al.	
120	20050266825		2005-12-01	CLAYTON, Steve	
121	20050266880		2005-12-01	GUPTA, Vivek G.	
122	20060014519		2006-01-19	MARSH et al.	
123	20060019632		2006-01-26	CUNNINGHAM et al.	
124	20060020787	A1	2006-01-26	Choyi et al.	
125	20060026679	A1	2006-02-02	Zakas	
126	20060030306	A1	2006-02-09	Kuhn, Brian Gerald	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	127	20060034256		2006-02-16	ADDAGATLA et al.	
	128	20060035631	A1	2006-02-16	White et al.	
	129	20060040642		2006-02-23	BORIS et al.	
	130	20060045245		2006-03-02	AARON et al.	
	131	20060048223		2006-03-02	LEE et al.	
	132	20060068796	A	2006-03-30	Millen, Stephanie L. et al.	
	133	20060072451	A1	2006-04-06	Ross, Alan D.	
	134	20060072550	A1	2006-04-06	Davis et al.	
	135	20060072646		2006-04-06	FEHER, Kamilo	
	136	20060075506	A1	2006-04-06	Sanda et al.	
	137	20060085543		2006-04-20	HRASTAR et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

138	20060095517	A1	2006-05-04	O'Connor et al.	
139	20060098627	A1	2006-05-11	Karaoguz et al.	
140	20060099970	A1	2006-05-11	Morgan et al.	
141	20060101507	A1	2006-05-11	Camenisch, Ja L.	
142	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
143	20060114821	A1	2006-06-01	Willey et al.	
144	20060114832	A	2006-06-01	Hamilton et al.	
145	20060126562	A1	2006-06-15	Liu, Huitao	
146	20060135144	A	2006-06-22	Jothipragasam, Premkumar	
147	20060136882	A1	2006-06-22	Noonan et al.	
148	20060143066	A1	2006-06-29	Calabria	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	149	20060143098		2006-06-29	LAZARIDIS, Mihal	
	150	20060156398	A	2006-07-13	Ross et al.	
	151	20060160536	A	2006-07-20	Chou, Joey	
	152	20060165060		2006-07-27	DUA, Robin	
	153	20060168128	A	2006-07-27	Sistla et al.	
	154	20060173959	A	2006-08-03	Mckelvie et al.	
	155	20060174035	A	2006-08-03	Tufail, Mudassir	
	156	20060178917		2006-08-10	MERRIAM et al.	
	157	20060178918		2006-08-10	MIKURAK, Michael G.	
	158	20060182137	A1	2006-08-17	Zhou et al.	
	159	20060183462		2006-08-17	KOLEHMAINEN, Mikko	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	160	20060190314		2006-08-24	HERNANDEZ, Rick	
	161	20060190987	A1	2006-08-24	Ohta et al.	
	162	20060193280	A1	2006-08-31	Lee et al.	
	163	20060199608		2006-09-07	DUNN et al.	
	164	20060200663	A1	2006-09-07	Thornton, Andrew J.	
	165	20060206709	A1	2006-09-14	Labrou et al.	
	166	20060206904		2006-09-14	WATKINS et al.	
	167	20060218395		2006-09-28	MAES, Stephane H.	
	168	20060233108		2006-10-19	KRISHNAN, Murali R.	
	169	20060233166		2006-10-19	BOU-DIAB et al.	
	170	20060236095		2006-10-19	SMITH et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

171	20060242685		2006-10-26	HEARD et al.	
172	20060258341		2006-11-16	MILLER et al.	
173	20060277590	A1	2006-12-07	Limont et al.	
174	20060291419	A1	2006-12-28	McConnell et al.	
175	20060291477		2006-12-28	CROAK et al.	
176	20070005795	A1	2007-01-04	Gonzalez, Ruben	
177	20070019670		2007-01-25	FALARDEAU, Eric	
178	20070022289		2007-01-25	ALT et al.	
179	20070025301	A	2007-02-01	Petersson et al.	
180	20070033194	A	2007-02-08	Srinivas et al.	
181	20070033197	A	2007-02-08	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	182	20070036312		2007-02-15	CAI et al.	
	183	20070055694		2007-03-08	RUGE et al.	
	184	20070060200	A1	2007-03-15	Boris et al.	
	185	20070061243	A1	2007-03-15	Ramer et al.	
	186	20070061800	A1	2007-03-15	Cheng et al.	
	187	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	188	20070073899	A1	2007-03-29	Judge et al.	
	189	20070076616		2007-04-05	NGO et al.	
	190	20070093243		2007-04-26	KAPADEKAR et al.	
	191	20070100981		2007-05-03	ADAMCZYK et al.	
	192	20070101426		2007-05-03	LEE et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	193	20070104126		2007-05-10	CALHOUN et al.	
	194	20070109983	A	2007-05-17	Shankar, Rohit et al.	
	195	20070111740	A1	2007-05-17	Wandel	
	196	20070124077	A1	2007-05-31	Hedlund	
	197	20070130283	A1	2007-06-07	Klein et al.	
	198	20070130315	A1	2007-06-07	Friend et al.	
	199	20070140113	A1	2007-06-21	Germelos	
	200	20070140145	A	2007-06-21	Kumar et al.	
	201	20070140275		2007-06-21	BOWMAN et al.	
	202	20070143824	A1	2007-06-21	Shahbazi, Majid	
	203	20070147317	A	2007-06-28	Smith et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	204	20070147324		2007-06-28	McGary, Faith	
	205	20070155365	A	2007-07-05	Kim, Sung-Jun et al.	
	206	20070165630	A1	2007-07-19	Rasanen et al.	
	207	20070168499	A	2007-07-19	Chu, Jing-Long	
	208	20070171856	A1	2007-07-26	Bruce et al.	
	209	20070174490	A1	2007-07-26	Choi et al.	
	210	20070191006	A1	2007-08-16	Carpenter	
	211	20070192460	A1	2007-08-16	Choi et al.	
	212	20070198656		2007-08-23	MAZZAFERRI et al.	
	213	20070201502	A1	2007-08-30	Abramson, Nathan	
	214	20070213054	A1	2007-09-13	Han, Seung-Wook	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	215	20070220251		2007-09-20	ROSENBERG et al.	
	216	20070226225		2007-09-27	YIU et al.	
	217	20070226775	A	2007-09-27	Andreasen et al.	
	218	20070234402	A1	2007-10-04	Khosravi et al.	
	219	20070242659	A1	2007-10-18	Cantu et al.	
	220	20070243862		2007-10-18	COSKUN et al.	
	221	20070248100	A1	2007-10-25	Zuberi et al.	
	222	20070254646	A1	2007-11-01	Sokondar	
	223	20070254675		2007-11-01	ZORLU OZER et al.	
	224	20070255769	A1	2007-11-01	Agrawal et al.	
	225	20070255797	A1	2007-11-01	Dunn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	226	20070255848		2007-11-01	SEWALL et al.	
	227	20070257767	A1	2007-11-08	Beeson, Curt	
	228	20070259656	A	2007-11-08	Jeong, Jong Woo	
	229	20070259673		2007-11-08	WILLARS et al.	
	230	20070263558		2007-11-15	SALOMONE, Leonardo	
	231	20070266422	A1	2007-11-15	Germano et al.	
	232	20070274327		2007-11-29	KAARELA et al.	
	233	20070280453		2007-12-06	Kelley, Sean S.	
	234	20070282896		2007-12-06	WYDROUG et al.	
	235	20070293191	A1	2007-12-20	Mir et al.	
	236	20070294395		2007-12-20	STRUB et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	237	20070294410	A1	2007-12-20	Pandya et al.	
	238	20070297378	A1	2007-12-27	Poyhonen et al.	
	239	20070298764		2007-12-27	CLAYTON, Steve	
	240	20070299965	A1	2007-12-27	Nieh et al.	
	241	20070300252		2007-12-27	Acharya, Swarup et al.	
	242	20080005285		2008-01-03	ROBINSON et al.	
	243	20080005561		2008-01-03	BROWN et al.	
	244	20080010379	A	2008-01-10	Zhao, Hang	
	245	20080010452		2008-01-10	HOLTZMAN et al.	
	246	20080018494	A1	2008-01-24	Waite et al.	
	247	20080022354	A	2008-01-24	Grewal, Karanvir et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

248	20080025230	A	2008-01-31	Patel et al.	
249	20080032715	A1	2008-02-07	Jia et al.	
250	20080034063	A1	2008-02-07	Yee, Robert	
251	20080034419	A	2008-02-07	Mullick et al.	
252	20080039102		2008-02-14	SEWALL et al.	
253	20080049630		2008-02-28	KOZISEK et al.	
254	20080050715	A1	2008-02-28	Golczewski et al.	
255	20080051076		2008-02-28	O'Shaughnessy, John et al.	
256	20080052387		2008-02-28	HEINZ et al.	
257	20080056273	A	2008-03-06	Pelletier et al.	
258	20080059474		2008-03-06	LIM, Keng	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	259	20080059743		2008-03-06	BYCHKOV et al.	
	260	20080060066		2008-03-06	WYNN et al.	
	261	20080062900		2008-03-13	RAO, Bindu Rama	
	262	20080064367		2008-03-13	NATH et al.	
	263	20080066149		2008-03-13	LIM, Keng	
	264	20080066150		2008-03-13	LIM, Keng	
	265	20080066181	A1	2008-03-13	Haveson et al.	
	266	20080070550	A	2008-03-20	Hose, David Alan	
	267	20080077705	A1	2008-03-27	Li et al.	
	268	20080080457	A1	2008-04-03	Cole, Terry L.	
	269	20080081606		2008-04-03	COLE, Terry L.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

270	20080082643		2008-04-03	STORRIE et al.	
271	20080083013		2008-04-03	SOLIMAN et al.	
272	20080085707		2008-04-10	FADELL, Tony	
273	20080089295	A	2008-04-17	Keeler, James D. et al.	
274	20080089303	A1	2008-04-17	Wirtanen et al.	
275	20080095339		2008-04-24	ELLIOTT et al.	
276	20080096559	A1	2008-04-24	Phillips et al.	
277	20080098062		2008-04-24	BALIA, Hinal K.	
278	20080109679		2008-05-08	WRIGHT et al.	
279	20080120129	A	2008-05-22	Seubert et al.	
280	20080120668		2008-05-22	Yau, Frank Chuen-Foo	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	281	20080120688		2008-05-22	QIU et al.	
	282	20080125079	A1	2008-05-29	O'Neil et al.	
	283	20080126287	A1	2008-05-29	Cox et al.	
	284	20080127304	A1	2008-05-29	Ginter et al.	
	285	20080130534		2008-06-05	TOMIOKA, Tazuko	
	286	20080130656		2008-06-05	KIM et al.	
	287	20080132201		2008-06-05	KARLBERG, Johan	
	288	20080132268	A1	2008-06-05	Choi-Grogan et al.	
	289	20080134330		2008-06-05	KAPOOR et al.	
	290	20080139210	A	2008-06-12	Gisby et al.	
	291	20080147454		2008-06-19	WALKER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	292	20080160958		2008-07-03	ABICHANDANI et al.	
	293	20080162637		2008-07-03	ADAMCZYK et al.	
	294	20080162704		2008-07-03	POPLETT et al.	
	295	20080164304		2008-07-10	NARASIMHAN et al.	
	296	20080166993	A1	2008-07-10	Gautier et al.	
	297	20080167027		2008-07-10	GAUTIER et al.	
	298	20080167033		2008-07-10	BECKERS, Michel	
	299	20080168275	A1	2008-07-10	DeAtley et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2688553	CA	A1	2008-12-04	Yoggie Security Systems, Inc.		☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

2	101035308	CN	A	2006-03-09	Huawei Tech. Co. Ltd.	☐
3	101080055	CN	A	2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.	☐
4	101115248	CN	A	2008-01-30	Lenovo Beijing Ltd.	☐
5	101123553	CN	A	2007-09-11	SouTheast University	☐
6	101127988	CN	A	2008-02-20	ZTE Corporation	☐
7	101155343	CN	B	2006-09-29	Huawei Tech. Co. Ltd.	☐
8	101183958	CN	A	2008-05-21	Huawei Tech. Co. Ltd.	☐
9	101335666	CN	A	2008-12-31	Hangzhou H3C Technologies Co., Ltd.	☐
10	101341764	CN	A	2009-01-07	Telefonaktiebolaget LM Ericsson	☐
11	101815275	CN	A	2010-08-25	Yang, Liu	☐
12	1310401	CN	A	2001-08-29	Wang, Di Xing	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

13	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.	☐
14	1508734	CN	A	2004-06-30	Chinese Creative Corp.	☐
15	1538730	CN	A	2004-10-20	Zhongxing Communication Co., Ltd.	☐
16	1567818	CN	A	2005-01-19	Huawei Tech. Co. Ltd.	☐
17	1801829	CN	A	2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.	☐
18	1802839	CN	A	2006-07-12	Motorola Inc.	☐
19	1867024	CN	A	2006-11-22	Huawei Technologies Co., Ltd.	☐
20	1878160	CN	A	2006-12-13	Huawei Technologies Co., Ltd.	☐
21	1889777	CN	A	2006-07-19	Huawei Tech. Co. Ltd.	☐
22	1937511	CN	A	2007-03-28	ZTE	☐
23	1098490	EP	A2	2001-05-09	Nortel Networks Ltd.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

24	1289326	EP	A1	2003-03-05	Motorola, Inc.	☐
25	1463238	EP		2004-09-29	Alcatel	☐
26	1503548	EP	A1	2005-02-02	FG Microtec GmbH	☐
27	1545114	EP	A1	2005-06-22	Alcatel	☐
28	1739518	EP		2007-01-03	Research In Motion Limited	☐
29	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.	☐
30	1850575	EP	A1	2007-10-31	Research In Motion	☐
31	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.	☐
32	1942698	EP	A1	2008-07-09	Apple Inc.	☐
33	1978772	EP		2008-10-08	British Telecommunications Public Limited Company	☐
34	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

35	2026514	EP	A1	2009-02-18	Nokia Siemens Networks	☐
36	2005339247	JP	A	2005-12-08	Secured Communications	☐
37	2006041989	JP		2006-02-09	Fujitsu Ltd.	☐
38	2006155263	JP	A	2006-06-15	NEC Corporation	☐
39	2006197137	JP		2006-07-27	NTT Docomo Inc.	☐
40	2006344007	JP	A	2006-12-21	Hitachi Ltd.	☐
41	2007318354	JP	A	2007-12-06	Fujitsu Ten Ltd.	☐
42	2008301121	JP	A	2008-12-11	Kyocera Corp.	☐
43	2009111919	JP		2009-05-21	Kyocera Communications Systems	☐
44	2009212707	JP	A	2009-09-17	Fujitsu Ltd.	☐
45	2009218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1		

	46	2009232107	JP	A	2009-10-08	Fujitsu Ltd.		☐
	47	3148713	JP	B2	2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		☐
	48	20040053858	KR	A	2004-06-25	Electronics and Telecommunications Research Instit		☐
	49	0208863	WO		2002-01-31	Telemac Corp.		☐
	50	1998058505	WO		1998-12-23	Sonera Oy		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	"Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	☐
	2	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐
	3	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐
	4	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

5	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	☐
6	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	☐
7	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," Release 8, Document No. 3GPP TS 23.401, V8.4.0, December 2008	☐
8	3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture," Release 8, Document No. 3GPP TS 23.203, V8.4.0, December 2008	☐
9	Ahmed et al., "A Context-Aware Vertical Handover Decision Algorithm for Multimode Mobile Terminals and its Performance," BenQ Mobile, Munich Germany; University of Klagenfurt, Klagenfurt, Austria; 2006	☐
10	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	☐
11	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	☐
12	Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009	☐
13	ANTON, B. et al., "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming"; Release Date February 2003; Version 1.0; Wi-Fi Alliance – Wireless ISP Roaming (WISPr)	☐
14	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	☐
15	BYRD, "Open Secure Wireless," May 5, 2010	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

16	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 26, 2008	☐
17	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	☐
18	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	☐
19	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	☐
20	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	☐
21	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	☐
22	Droid Wall 1.3.7 description 20100428 obtained from https://www.freewarelovers.com/android/apps/droid-wall	☐
23	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	☐
24	European Commission, "Data Roaming Tariffs - Transparency Measures," obtained from EUROPA - Europe's Information Society Thematic Portal website, June 24, 2011: " http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm ."	☐
25	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	☐
26	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

27	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	☐
28	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	☐
29	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	☐
30	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	☐
31	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	☐
32	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	☐
33	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	☐
34	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	☐
35	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	☐
36	Koutsopoulou et al., "Charging, Accounting and Billing Management Schemes in Mobile Telecommunication Networks and the Internet," IEEE Communications Surveys & Tutorials, First Quarter 2004, Vol. 6, No. 1	☐
37	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

38	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	☐
39	KYRIAKAKOS et al., "Ubiquitous Service Provision in Next Generation Mobile Networks," Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	☐
40	Li, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	☐
41	Loopt User Guide, metroPCS, 7/17/2008	☐
42	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	☐
43	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	☐
44	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	☐
45	Nuzman et al., "A compound model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	☐
46	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	☐
47	OPPLIGER, Rolf, "Internet Security: Firewalls and Beyond," Communications of the ACM, May 1997, Vol. 40, No. 5	☐
48	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2414	
	Examiner Name	NOT YET ASSIGNED	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

49	Richtel, "Cellphone consumerism; If even a debit card is too slow, now you have a new way to act on impulse: [National Edition]," National Post, Canada, Oct. 2, 2007	☐
50	Rivadeneira et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	5131020	A	1992-07-14	Liebesny et al.	
	2	5283904		1994-02-01	CARSON, David G. et al.	
	3	5325532	A	1994-06-28	Crosswy et al.	
	4	5572528	A	1996-11-05	Shuen, Pauline	
	5	5577100	A	1996-11-19	McGregor et al.	
	6	5594777		1997-01-14	Makkonen, Matti et al.	
	7	5617539	A	1997-04-01	Ludwig et al.	
	8	5630159	A	1997-05-13	Zancho, William F.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	9	5633484	A	1997-05-27	Zancho, William F. et al.	
	10	5633868	A	1997-05-27	Baldwin et al.	
	11	5751719	A	1998-05-12	Chen et al.	
	12	5754953	A	1998-05-19	Briancon et al.	
	13	5774532	A	1998-06-30	Gottlieb et al.	
	14	5794142		1998-08-11	VANTTILA et al.	
	15	5814798	A	1998-09-29	Zancho, William F.	
	16	5889477		1999-03-30	Fastenrath, Ulrich	
	17	5892900		1999-04-06	GINTER et al.	
	18	5903845		1999-05-11	BUHRMANN et al.	
	19	5915008	A	1999-06-22	Dulman, Scott	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

20	5915226	A	1999-06-22	Martineau	
21	5933778		1999-08-03	BUHRMANN et al.	
22	5940472		1999-08-17	NEWMAN et al.	
23	5974439	A	1999-10-26	Boliella, Gregory	
24	5983270	A	1999-11-09	Abraham et al.	
25	6035281		2000-03-07	Crosskey, James P. et al.	
26	6038452		2000-03-14	Strawczynski, Leo et al.	
27	6038540	A	2000-03-14	Krist et al.	
28	6047268		2000-04-04	BARTOLI et al.	
29	6058434	A	2000-05-02	Wilt et al.	
30	6061571	A	2000-05-09	Tamura, Hideo	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

31	6064878		2000-05-16	DENKER, John Stewart et al.	
32	6078953		2000-06-20	VAID et al.	
33	6081591		2000-06-27	SKOOG, Frederick H.	
34	6098878		2000-08-08	DENT et al.	
35	6104700	A	2000-08-15	Haddock, Stephen R. et al.	
36	6115823	A	2000-09-05	Velasco et al.	
37	6119933	A	2000-09-19	Wong et al.	
38	6125391	A	2000-09-26	Meltzer et al.	
39	6141565	A	2000-10-31	Feuerstein et al.	
40	6141686		2000-10-31	JACKOWSKI et al.	
41	6148336		2000-11-14	THOMAS et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	6154738		2000-11-28	CALL, Charles Gainor	
43	6157636	A	2000-12-05	Voit et al.	
44	6185576	B1	2001-02-06	Mcintosh, Lowrie	
45	6198915		2001-03-06	McGREGOR et al.	
46	6219786	B1	2001-04-17	Cunningham et al.	
47	6226277		2001-05-01	Chuah, Mooi Choo	
48	6246870	B1	2001-06-12	Dent et al.	
49	6263055		2001-07-17	GARLAND et al.	
50	6292828		2001-09-18	Williams, David L.	
51	6317584		2001-11-13	ABU-AMARA et al.	
52	6370139	B2	2002-04-09	Redmond	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	6381316		2002-04-30	JOYCE, Simon James et al.	
54	6393014	B1	2002-05-21	Daly et al.	
55	6397259	B1	2002-05-28	Lincke et al.	
56	6401113	B2	2002-06-04	Lazaridis et al.	
57	6418147		2002-07-09	WIEDEMAN, Robert A.	
58	6438575	B1	2002-08-20	Khan et al.	
59	6445777	B1	2002-09-03	Clark, Curtis	
60	6449479		2002-09-10	SANCHEZ, Eduardo	
61	6466984	B1	2002-10-15	Naveh et al.	
62	6477670		2002-11-05	Ahmadvand, Nima	
63	6502131		2002-12-31	VAID, Aseem et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

64	6505114		2003-01-07	LUCIANI, Sergio	
65	6510152	B1	2003-01-21	Gerszberg et al.	
66	6522629	B1	2003-02-18	Anderson, Sr., Ronald D.	
67	6532235		2003-03-11	BENSON et al.	
68	6532579		2003-03-11	SATO et al.	
69	6535855	B1	2003-03-18	Cahill et al.	
70	6535949	B1	2003-03-18	Parker, Kenneth W.	
71	6539082		2003-03-25	LOWE et al.	
72	6542500	B1	2003-04-01	Gerszberg et al.	
73	6542992		2003-04-01	Peirce, Kenneth L. et al.	
74	6546016	B1	2003-04-08	Gerszberg et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

75	6563806		2003-05-13	YANO et al.	
76	6570974	B1	2003-05-27	Gerszberg et al.	
77	6574321		2003-06-03	COX et al.	
78	6574465		2003-06-03	MARSH et al.	
79	6578076	B1	2003-06-10	Putzolu, David Matthew	
80	6581092		2003-06-17	MOTOYAMA, Tetsuro	
81	6591098	B1	2003-07-08	Shieh et al.	
82	6598034	B1	2003-07-22	Kloth, Axel K.	
83	6601040	B1	2003-07-29	Kolis, H. Brock	
84	6603969		2003-08-05	VUORISTO et al.	
85	6603975	B1	2003-08-05	Inouchi et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

86	6606744		2003-08-12	MIKURAK, Michael G.	
87	6628934	A	2003-09-30	Rosenberg et al.	
88	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
89	6636721	B2	2003-10-21	Threadgill et al.	
90	6639975	B1	2003-10-28	O'Neal et al.	
91	6640097		2003-10-28	Corrigan, Louis et al.	
92	6640334	B	2003-10-28	Rasmussen, John H.	
93	6650887		2003-11-18	McGREGOR et al.	
94	6651101		2003-11-18	GAI et al.	
95	6654786	B1	2003-11-25	Fox et al.	
96	6654814		2003-11-25	Britton, Kathryn H. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

97	6658254		2003-12-02	PURDY et al.	
98	6662014	B1	2003-12-09	Walsh, Patrick Jay	
99	6678516	B2	2004-01-13	Nordman et al.	
100	6683853		2004-01-27	Kannas, Chris et al.	
101	6684244		2004-01-27	GOLDMAN et al.	
102	6690918	B2	2004-02-10	Evans et al.	
103	6697821	B2	2004-02-24	Ziff et al.	
104	6725031		2004-04-20	WATLER et al.	
105	6725256	B1	2004-04-20	Alibal et al.	
106	6732176	B1	2004-05-04	Stewart et al.	
107	6735206	B1	2004-05-11	Oki et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	108	6748195	B1	2004-06-08	Phillips, W. Gariand	
	109	6748437	B1	2004-06-08	Mankude et al.	
	110	6751296	B1	2004-06-15	Albal et al.	
	111	6754470		2004-06-22	Hendrickson, Keith et al.	
	112	6757717	B1	2004-06-29	Goldstein, Leonid	
	113	6760417	B1	2004-07-06	Wallenius, Jukka	
	114	6763000		2004-07-13	WALSH, Peter J.	
	115	6763226	B1	2004-07-13	McZeal Jr., Alfred	
	116	6765864		2004-07-20	NATARAJAN et al.	
	117	6765925		2004-07-20	Sawyer, Wilson et al.	
	118	6782412		2004-08-24	BROPHY, Kevin et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	119	6785889		2004-08-31	WILLIAMS, Peter	
	120	6792461	B1	2004-09-14	Hericourt, Olivier	
	121	6829596		2004-12-07	FRAZEE, Steve	
	122	6829696		2004-12-07	BALMER et al.	
	123	6839340		2005-01-04	Voit, Eric A. et al.	
	124	6842628	B1	2005-01-11	Arnold et al.	
	125	6873988	B2	2005-03-29	Herrmann et al.	
	126	6876653		2005-04-05	AMBE, Shekhar et al.	
	127	6879825	B1	2005-04-12	Daly, Brian Kevin	
	128	6882718	B1	2005-04-19	Smith, Benjamin V.	
	129	6885997	B1	2005-04-26	Roberts, David T.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

130	6901440	B1	2005-05-31	Bimm et al.	
131	6920455		2005-07-19	WESCHLER, Paul	
132	6922562		2005-07-26	Ward, Stephen L. et al.	
133	6928280		2005-08-09	Xanthos, James et al.	
134	6934249	B1	2005-08-23	Bertin, Olivier et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20080168523		2008-07-10	ANSARI et al.	
	2	20080177998		2008-07-24	APSANGI et al.	
	3	20080178300	A1	2008-07-24	Brown et al.	
	4	20080183811	A1	2008-07-31	Kotras et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

5	20080183812		2008-07-31	PAUL et al.	
6	20080184127		2008-07-31	RAFEY et al.	
7	20080189760		2008-08-07	ROSENBERG et al.	
8	20080201266	A	2008-08-21	Chua et al.	
9	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
10	20080212470		2008-09-04	CASTANEDA et al.	
11	20080212751	A1	2008-09-04	Chung, Simon	
12	20080219268		2008-09-11	DENNISON, Larry R.	
13	20080221951		2008-09-11	STANFORTH et al.	
14	20080222692		2008-09-11	ANDERSSON et al.	
15	20080225748		2008-09-18	KHEMANI et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

16	20080229385		2008-09-18	FEDER et al.	
17	20080229388		2008-09-18	MAES, Stephane H.	
18	20080235511		2008-09-25	O'BRIEN, William G. et al.	
19	20080240373		2008-10-02	WILHELM, Robert D.	
20	20080250053	A	2008-10-09	Aaltonen, Janne et al.	
21	20080256593		2008-10-16	VINBERG et al.	
22	20080259924	A1	2008-10-23	Gooch et al.	
23	20080262798		2008-10-23	KIM, Eun Ah et al.	
24	20080263348	A	2008-10-23	Zaltsman et al.	
25	20080268813		2008-10-30	MAES, Stephane H.	
26	20080270212	A	2008-10-30	Blight et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

27	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
28	20080282319	A1	2008-11-13	Fontijn et al.	
29	20080293395	A1	2008-11-27	Mathews et al.	
30	20080298230		2008-12-04	LUFT et al.	
31	20080305793		2008-12-11	GALLAGHER et al.	
32	20080311885		2008-12-18	DAWSON et al.	
33	20080313315	A	2008-12-18	Karaoguz et al.	
34	20080313730		2008-12-18	Iftimie, Sorin et al.	
35	20080316923		2008-12-25	FEDDERS et al.	
36	20080318547		2008-12-25	BALLOU et al.	
37	20080318550		2008-12-25	DeATLEY, Dallas	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

38	20080319879		2008-12-25	CARROLL et al.	
39	20080320497	A1	2008-12-25	Tarkoma et al.	
40	20090005000	A	2009-01-01	Baker, Matthew et al.	
41	20090005005		2009-01-01	FORSTALL et al.	
42	20090006116	A	2009-01-01	Baker, Matthew et al.	
43	20090006200	A	2009-01-01	Baker, Matthew et al.	
44	20090006229	A1	2009-01-01	Sweeney et al.	
45	20090013157		2009-01-08	BEAULE, Stephane	
46	20090016310	A1	2009-01-15	Rasal, Digambar L.	
47	20090036111	A1	2009-02-05	Danford et al.	
48	20090042536	A1	2009-02-12	Bernard et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

49	20090044185	A1	2009-02-12	Krivopaltsev, Eugene	
50	20090046707	A1	2009-02-19	Smires et al.	
51	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
52	20090047989	A1	2009-02-19	Harmon et al.	
53	20090048913	A1	2009-02-19	Shenfield et al.	
54	20090049156	A1	2009-02-19	Aronsson et al.	
55	20090049518	A1	2009-02-19	Roman et al.	
56	20090054030		2009-02-26	GOLDS, David	
57	20090065571	A1	2009-03-12	Jain, Deepak	
58	20090067372		2009-03-12	SHAH, Keyur C. et al.	
59	20090068984		2009-03-12	BURNETT, R. Alan	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

60	20090070379	A1	2009-03-12	Rappaport, Theodore R.	
61	20090077622		2009-03-19	BAUM et al.	
62	20090079699		2009-03-26	SUN, Jian	
63	20090113514		2009-04-30	HU, Q. James	
64	20090125619		2009-05-14	ANTANI, Snehal S.	
65	20090132860	A1	2009-05-21	LIU et al.	
66	20090149154	A1	2009-06-11	Bhasin et al.	
67	20090157792	A1	2009-06-18	Fiatal	
68	20090163173	A1	2009-06-25	Williams, Timothy D.	
69	20090172077		2009-07-02	ROXBURGH, David et al.	
70	20090180391		2009-07-16	PETERSEN et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

71	20090181662	A1	2009-07-16	Fleischman et al.	
72	20090197585		2009-08-06	AARON, Jeffrey A.	
73	20090197612	A1	2009-08-06	Kiiskinen, Arto	
74	20090203352	A1	2009-08-13	Fordon et al.	
75	20090217364	A1	2009-08-27	Salmela et al.	
76	20090219170		2009-09-03	CLARK, Ryan C. et al.	
77	20090248883		2009-10-01	SURYANARAYANA et al.	
78	20090254857	A	2009-10-08	Romine et al.	
79	20090257379		2009-10-15	ROBINSON et al.	
80	20090271514		2009-10-29	THOMAS et al.	
81	20090282127	A	2009-11-12	Leblanc et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		17577237
Filing Date		2022-01-17
First Named Inventor	RALEIGH, GREGORY	
Art Unit	2414	
Examiner Name	NOT YET ASSIGNED	
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	82	20090286507		2009-11-19	O'NEIL et al.	
	83	20090287921		2009-11-19	ZHU et al.	
	84	20090288140	A1	2009-11-19	Huber et al.	
	85	20090291665	A1	2009-11-26	Gaskarth et al.	
	86	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	87	20090307696	A1	2009-12-10	Vais et al.	
	88	20090307746	A1	2009-12-10	DI et al.	
	89	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	90	20090320110	A1	2009-12-24	NICOLSON et al.	
	91	20100017506		2010-01-21	FADELL, Anthony	
	92	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

93	20100027469	A1	2010-02-04	Gurajala et al.	
94	20100027559		2010-02-04	LIN, Hung-Ming et al.	
95	20100030890	A	2010-02-04	Dutta et al.	
96	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
97	20100041365	A1	2010-02-18	Lott et al.	
98	20100042675		2010-02-18	FUJII, Hiroshi	
99	20100043068		2010-02-18	VARADHAN et al.	
100	20100069074	A1	2010-03-18	Kodialam et al.	
101	20100071053		2010-03-18	ANSARI et al.	
102	20100075666	A1	2010-03-25	Garner, Neil Robert	
103	20100077035	A1	2010-03-25	Li et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	104	20100080202		2010-04-01	Hanson, Mark	
	105	20100082431		2010-04-01	RAMER et al.	
	106	20100088387	A1	2010-04-08	Calamera	
	107	20100103820		2010-04-29	FULLER et al.	
	108	20100113020	A1	2010-05-06	Subramanian et al.	
	109	20100121744	A1	2010-05-13	Beiz et al.	
	110	20100131584		2010-05-27	Johnson, William J.	
	111	20100142478	A1	2010-06-10	Forssell et al.	
	112	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	113	20100151866	A1	2010-06-17	Karpov et al.	
	114	20100153781		2010-06-17	HANNA, Stephen R.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

115	20100167696	A	2010-07-01	Smith, Christopher David et al.	
116	20100188975		2010-07-29	RALEIGH, Gregory G.	
117	20100188990		2010-07-29	RALEIGH, Gregory G.	
118	20100188992		2010-07-29	RALEIGH, Gregory G.	
119	20100188994		2010-07-29	RALEIGH, Gregory G.	
120	20100190469	A1	2010-07-29	Vanderveen et al.	
121	20100191576		2010-07-29	RALEIGH, Gregory G.	
122	20100191612		2010-07-29	RALEIGH, Gregory G.	
123	20100191846		2010-07-29	RALEIGH, Gregory G.	
124	20100192170		2010-07-29	RALEIGH, Gregory G.	
125	20100192212		2010-07-29	RALEIGH, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	126	20100195503		2010-08-05	RALEIGH, Gregory G.	
	127	20100197268		2010-08-05	RALEIGH, Gregory G.	
	128	20100198698		2010-08-05	RALEIGH et al.	
	129	20100198939		2010-08-05	RALEIGH, Gregory G.	
	130	20100241544		2010-09-23	Benson, Dan et al.	
	131	20100248719	A1	2010-09-30	Scholaert, Hugh	
	132	20100284327	A	2010-11-11	Miklos, Gyorgy	
	133	20100284388	A1	2010-11-11	Fantini et al.	
	134	20100287599	A1	2010-11-11	He et al.	
	135	20100325420		2010-12-23	KANEKAR, Tushar	
	136	20110004917	A1	2011-01-06	Saisa et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	137	20110013569	A	2011-01-20	Scherzer, Shimon et al.	
	138	20110019574	A	2011-01-27	Malomsoky et al.	
	139	20110081881	A	2011-04-07	Baker, Matthew Donald et al.	
	140	20110082790	A	2011-04-07	Baker, Matthew Donald et al.	
	141	20110110309	A	2011-05-12	Bennett, James D.	
	142	20110126141		2011-05-26	KING et al.	
	143	20110145920	A1	2011-06-16	Mahaffey et al.	
	144	20110159818	A	2011-06-30	Scherzer, Shimon et al.	
	145	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	146	20110185202	A1	2011-07-28	Black et al.	
	147	20110244837	A1	2011-10-06	MURATA et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

148	20110249668	A1	2011-10-13	Milligan et al.	
149	20110264923	A	2011-10-27	Kocher et al.	
150	20120020296	A	2012-01-26	Scherzer, Shimon et al.	
151	20120144025	A1	2012-06-07	Melander et al.	
152	20120166364	A1	2012-06-28	Ahmad et al.	
153	20120196644	A	2012-08-02	Scherzer, Shimon et al.	
154	20120238287	A	2012-09-20	Scherzer, Shimon	
155	20130029653	A	2013-01-31	Baker, Matthew Donald et al.	
156	20130058274	A	2013-03-07	Scherzer, Shimon et al.	
157	20130065555	A	2013-03-14	Baker, Matthew Donald et al.	
158	20130072177	A1	2013-03-21	Ross et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	159	20130084835	A	2013-04-04	Scherzer, Shimon et al.	
	160	20130144789		2013-06-06	Aaltonen, Janne et al.	
	161	20130225151	A1	2013-08-29	King et al.	
	162	20130326356	A9	2013-12-05	Zheng et al.	
	163	20140073291	A1	2014-03-13	Hildner et al.	
	164	20140241342	A1	2014-08-28	Constantinof, Cristian	
	165	20150181628	A1	2015-06-25	Haverinen et al.	
	166	20200077892	A1	2020-03-12	Tran	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1999027723	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

2	1999065185	WO	A3	2001-05-03	Briscoe et al.	☐
3	2002045315	WO	A2	2002-06-06	Micromuse	☐
4	2002067616	WO	A1	2002-08-29	Sonera Oyj	☐
5	2002093877	WO	A1	2002-11-21	Nokia Corp.	☐
6	2003014891	WO		2003-02-20	The Boeing Company	☐
7	2003017063	WO	A2	2003-02-27	Apogee Networks	☐
8	2003017065	WO	A2	2003-02-27	Apogee Networks	☐
9	2003058880	WO	A1	2003-07-17	Eriksson et al.	☐
10	2004028070	WO	A1	2004-04-01	Mann et al.	☐
11	2004064306	WO	A2	2004-07-29	Wild et al.	☐
12	2004077797	WO	A3	2008-02-07	Erskine et al.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

13	2004095753	WO	A3	2005-01-13	Adwankar et al.	☐
14	2005008995	WO		2005-01-27	Starhub Ltd.	☐
15	2005053335	WO	A1	2005-06-09	Nokia Corp.	☐
16	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.	☐
17	2006004467	WO	A1	2006-01-12	Skog et al.	☐
18	2006004784	WO	A1	2006-01-12	Japan Communications Inc.	☐
19	2006012610	WO	A2	2006-02-02	Citrix Systems, Inc.	☐
20	2006050758	WO	A1	2006-05-18	Boman	☐
21	2006073837	WO	A3	2009-04-02	D'agostino, Anthony	☐
22	2006077481	WO	A1	2006-07-27	Chane et al.	☐
23	2006093961	WO	A1	2006-09-08	Kyocera Wireless Corp.	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		17577237
Filing Date		2022-01-17
First Named Inventor	RALEIGH, GREGORY	
Art Unit	2414	
Examiner Name	NOT YET ASSIGNED	
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	24	2006120558	WO		2006-11-16	Nokia Corp.		☐
	25	2006130960	WO	A1	2006-12-14	Sharif-Ahmadi et al.		☐
	26	2007001833	WO	A2	2007-01-04	Linsley-Hood et al.		☐
	27	2007014630	WO	A1	2007-02-08	Norrman et al.		☐
	28	2007018363	WO	A1	2007-02-15	Son		☐
	29	2007053848	WO	A1	2007-05-10	Germano et al.		☐
	30	2007068288	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		☐
	31	2007069245	WO	A3	2009-04-16	Touboul		☐
	32	2007097786	WO	A	2007-08-30	Sony Ericsson Mobile Communications AB		☐
	33	2007107701	WO	A2	2007-09-27	Cofta		☐
	34	2007120310	WO		2007-10-25	Qualcomm Inc.		☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		17577237
Filing Date		2022-01-17
First Named Inventor	RALEIGH, GREGORY	
Art Unit	2414	
Examiner Name	NOT YET ASSIGNED	
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

	35	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		☐
	36	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		☐
	37	2007129180	WO	A2	2007-11-15	Nokia Corp.		☐
	38	2007133844	WO	A	2007-11-22	Camiant, Inc.		☐
	39	2008017837	WO	A1	2008-02-14	Spooner		☐
	40	2008051379	WO	A2	2008-05-02	Balia		☐
	41	2008066419	WO	A1	2008-06-05	LIDSTRÖM et al.		☐
	42	2008080139	WO	A1	2008-07-03	Pugh et al.		☐
	43	2008080430	WO	A1	2008-07-10	Costa et al.		☐
	44	2008099802	WO	A1	2008-08-21	Awano		☐
	45	2009008817	WO	A1	2009-01-15	Ericsson		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	46	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson		☐
	47	2010088413	WO	A1	2010-08-05	Raleigh		☐
	48	2010128391	WO	A2	2010-11-11	Bridgewater Systems Corp.		☐
	49	2010128391	WO	A3	2011-01-20	Montahan et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	☐
	2	Sadeh et al., "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," ISR School of Computer Science, Carnegie Mellon University, 2007	☐
	3	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	☐
	4	SHARKEY, "Coding for Life--Battery Life, That Is," May 27, 2009	☐
	5	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1

6	Sun et al., "Towards Connectivity Management Adaptability: Context Awareness in Policy Representation and End-to-end Evaluation Algorithm," Dept. of Electrical and Information Engineering, Univ. of Oulu, Finland, 2004	☐
7	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	☐
8	VerizonWireless.com news, "Verizon Wireless Adds to Portfolio of Cosumer-Friendly Tools With Introduction of Usage Controls, Usage Controls and Chaperone 2.0 Offer Parents Full Family Security Solution," August 18, 2008	☐
9	Windows7 Power Management, published April 2009	☐
10	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	6934751	B2	2005-08-23	Jayapalan et al.	
	2	6947723		2005-09-20	Gurnani, Roger et al.	
	3	6947985	B2	2005-09-20	Hegli et al.	
	4	6952428		2005-10-04	NECKA et al.	
	5	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	6	6959202	B2	2005-10-25	Heinonen et al.	
	7	6959393	B2	2005-10-25	Hollis et al.	
	8	6965667		2005-11-15	TRABANDT et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

9	6965872		2005-11-15	Grdina, Jerome M.	
10	6967958		2005-11-22	ONO, Yoshiyuki et al.	
11	6970692	B2	2005-11-29	Tysor, Arthur James	
12	6970927	B1	2005-11-29	Stewart et al.	
13	6982733	B1	2006-01-03	McNaily et al.	
14	6983370	B2	2006-01-03	Eaton et al.	
15	6996062	B1	2006-02-07	Freed et al.	
16	6996076		2006-02-07	FORBES et al.	
17	6996393		2006-02-07	Pyhalammi, Seppo et al.	
18	6998985		2006-02-14	REISMAN et al.	
19	7002920		2006-02-21	Ayyagari, Deepak et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	20	7007295	B1	2006-02-28	Rose et al.	
	21	7013469	B2	2006-03-14	Smith et al.	
	22	7017189	B1	2006-03-21	DeMello et al.	
	23	7024200		2006-04-04	McKENNA et al.	
	24	7024460	B2	2006-04-04	Koopmas et al.	
	25	7027055	B2	2006-04-11	Anderson et al.	
	26	7027408		2006-04-11	NABKEL et al.	
	27	7031733	B2	2006-04-18	Aiminana et al.	
	28	7032072	B1	2006-04-18	Quinn et al.	
	29	7039027	B2	2006-05-02	Bridgelall, Raj	
	30	7039037		2006-05-02	Wang, Jiwei R. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	31	7039403		2006-05-02	Wong, Gregory A.	
	32	7039713	B1	2006-05-02	Van Gunter, David et al.	
	33	7042988		2006-05-09	JUITT et al.	
	34	7043225	B1	2006-05-09	Patel et al.	
	35	7043226		2006-05-09	Yamauchi, Toshiaki	
	36	7043268	B2	2006-05-09	Yukie et al.	
	37	7047276	B2	2006-05-16	Liu et al.	
	38	7058022	B1	2006-06-06	Caroian et al.	
	39	7058968		2006-06-06	ROWLAND et al.	
	40	7068600		2006-06-27	CAIN, Joseph Bibb	
	41	7069248		2006-06-27	HUBER, Adriano	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	7082422	B1	2006-07-25	Zirngibl et al.	
43	7084775	B1	2006-08-01	Smith, Michael R.	
44	7092696		2006-08-15	HOSAIN et al.	
45	7095754	B2	2006-08-22	Benveniste, Mathilde	
46	7102620	B2	2006-09-05	Harries, Andrew Stanely Guy et al.	
47	7110753	B2	2006-09-19	Campen, Kenneth Brian	
48	7113780	B2	2006-09-26	Mckenna Daniel et al.	
49	7113997		2012-09-26	Jayapalan, Jay et al.	
50	7120133	B1	2006-10-10	Joo et al.	
51	7133386	B2	2006-11-07	Holur et al.	
52	7133695	B2	2006-11-07	Beyda, William J.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	7136361	B2	2006-11-14	Benveniste, Mathilde	
54	7139569	B2	2006-11-21	Kato, Akira	
55	7142876		2006-11-28	TROSSEN et al.	
56	7149229	B1	2006-12-12	Leung, Kent K.	
57	7149521	B2	2006-12-12	Sundar et al.	
58	7151764	B1	2006-12-19	Heinonen et al.	
59	7158792		2007-01-02	COOK et al.	
60	7162237	B1	2007-01-09	Silver et al.	
61	7165040	B2	2007-01-16	Ehrman et al.	
62	7167078		2007-01-23	POURCHOT, Shawn C.	
63	7171199	B1	2007-01-30	Rahman	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

64	7174156	B1	2007-02-06	Mangai, Manish	
65	7174174		2007-02-06	BORIS et al.	
66	7177919	B1	2007-02-13	Truong et al.	
67	7180855		2007-02-20	LIN , Wei	
68	7181017		2007-02-20	Nagei, Robert H. et al.	
69	7191248	B2	2007-03-13	Chattopadhyay et al.	
70	7197321		2007-03-27	ERSKINE et al.	
71	7200112	B2	2007-04-03	Sundar et al.	
72	7200551	B1	2007-04-03	Senez	
73	7203169	B1	2007-04-10	Okholm, Jon et al.	
74	7203721	B1	2007-04-10	Ben-Efraim et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	75	7203752	B2	2007-04-10	Rice et al.	
	76	7212491		2007-05-01	Koga, Takahiro	
	77	7219123	B1	2007-05-15	Fiechter et al.	
	78	7222190	B2	2007-05-22	Klinker et al.	
	79	7222304	B2	2007-05-22	Beaton et al.	
	80	7224968	B2	2007-05-29	Dobson et al.	
	81	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	82	7236780		2007-06-26	Benco, David S.	
	83	7242668	B2	2007-07-10	Kan et al.	
	84	7242920		2007-07-10	MORRIS, Robert P.	
	85	7245901		2007-07-17	McGREGOR et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

86	7248570	B2	2007-07-24	Bahl et al.	
87	7248868	B2	2007-07-24	Snyder et al.	
88	7251218		2007-07-31	Jorgensen, Jacob W.	
89	7260382	B1	2007-08-21	Lamb et al.	
90	7266371	B1	2007-09-04	Amin et al.	
91	7269157	B2	2007-09-11	Klinker et al.	
92	7271765	B2	2007-09-18	Stilp et al.	
93	7272660	B1	2007-09-18	Powers et al.	
94	7280816		2007-10-09	FRATTI et al.	
95	7280818		2007-10-09	CLAYTON, Steve	
96	7283561		2007-10-16	Picher-Dempsey, Heidi	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

97	7283963		2007-10-16	FITZPATRICK, John E. et al.	
98	7286834	B2	2007-10-23	Walter	
99	7286848	B2	2007-10-23	Vireday, Richard P. et al.	
100	7289489		2007-10-30	KUNG et al.	
101	7290283		2007-10-30	COPELAND III, John A.	
102	7310424		2007-12-18	Gehring, Stephan Walter et al.	
103	7313237	B2	2007-12-25	Bahl, Paramvir et al.	
104	7315892	B2	2008-01-01	Freimuth et al.	
105	7317699		2008-01-08	GODFREY et al.	
106	7318111	B2	2008-01-08	Zhao, Wen	
107	7320029	B2	2008-01-15	Rinne et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	108	7322044		2008-01-22	HRASTAR, Scott E.	
	109	7324447		2008-01-29	MORFORD, Michael Robert	
	110	7325037		2008-01-29	LAWSON, Karen L.	
	111	7336960		2008-02-26	ZAVALKOVSKY et al.	
	112	7340772	B2	2008-03-04	Panasyuk et al.	
	113	7346410		2008-03-18	UCHIYAMA, Kenji	
	114	7349695		2008-03-25	OOMMEN et al.	
	115	7353533	B2	2008-04-01	Wright et al.	
	116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	117	7356337		2008-04-08	FLORENCE, Shahar	
	118	7366497		2008-04-29	NAGATA, Hideaki	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

119	7366654	B2	2008-04-29	Moore, Robert C.	
120	7369848	B2	2008-05-06	Jiang, Yue Jun	
121	7369856	B2	2008-05-06	Ovadia, Shlomo	
122	7373136		2008-05-13	WATLER et al.	
123	7373179		2008-05-13	Stine, Ted et al.	
124	7379731	B2	2008-05-27	Natsuno et al.	
125	7388950		2008-06-17	ELSEY et al.	
126	7389412	B2	2008-06-17	Sharma et al.	
127	7391724	B2	2008-06-24	Alakoski et al.	
128	7395244	B1	2008-07-01	Kingsford, Bryan	
129	7401338		2008-07-15	BOWEN et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	130	7403763		2008-07-22	MAES, Stephane H.	
	131	7409447	B	2008-08-05	Assadzadeh, Alireza	
	132	7409569	B2	2008-08-05	Illowsky et al.	
	133	7411930	B2	2008-08-12	Montejo et al.	
	134	7418253		2008-08-26	KAVANAHA, Alan	
	135	7418257		2008-08-26	Kim, Myong-Ju	
	136	7421004		2008-09-02	FEHER, Kamilo	
	137	7423971	B1	2008-09-09	Mohaban et al.	
	138	7428750	B1	2008-09-23	Dunn et al.	
	139	7433362	B2	2008-10-07	Mallya et al.	
	140	7436816	B2	2008-10-14	Mehta et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	141	7440433	B2	2008-10-21	Rink et al.	
	142	7444669	B1	2008-10-28	Bahl, Paramvir et al.	
	143	7450591		2008-11-11	KORLING et al.	
	144	7450927		2008-11-11	CRESWELL et al.	
	145	7454191	B2	2008-11-18	Dawson et al.	
	146	7457265		2008-11-25	Julka, Vibhor et al.	
	147	7457870	B1	2008-11-25	Lownsborough et al.	
	148	7460837	B2	2008-12-02	Diener, Neil R.	
	149	7466652	B2	2008-12-16	Lau et al.	
	150	7467160	B2	2008-12-16	McIntyre	
	151	7472189		2008-12-30	Mallya, Arvind R. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

152	7478420	B2	2009-01-13	Wright, Michael et al.	
153	7486185		2009-02-03	CULPEPPER et al.	
154	7486658	B2	2009-02-03	Kumar, Rajneesh	
155	7493659	B1	2009-02-17	Wu, Handong et al.	
156	7496652		2009-02-24	Pezzutti, David	
157	7499438		2009-03-03	Hinman, Brian L. et al.	
158	7499537		2009-03-03	ELSEY et al.	
159	7502672	B1	2009-03-10	Kolis, H. Brock	
160	7505756	B2	2009-03-17	Bahl	
161	7505795	B1	2009-03-17	Lim et al.	
162	7508799	B2	2009-03-24	Sumner et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

163	7512128	B2	2009-03-31	DiMambro et al.	
164	7512131	B2	2009-03-31	Svensson et al.	
165	7515608		2009-04-07	Yuan, Yuan et al.	
166	7515926	B2	2009-04-07	Bu et al.	
167	7516219		2009-04-07	MOGHADDAM et al.	
168	7522549	B2	2009-04-21	Karaoguz et al.	
169	7522576	B2	2009-04-21	Du et al.	
170	7526541	B2	2009-04-28	Roese et al.	
171	7529204	B2	2009-05-05	Bourlas, Yair et al.	
172	7535880		2009-05-19	Hinman, Brian L. et al.	
173	7536695	B2	2009-05-19	Alam et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

174	7539132	B2	2009-05-26	Werner et al.	
175	7539862	B2	2009-05-26	Edgett et al.	
176	7540408	B2	2009-06-02	Levine et al.	
177	7545782		2009-06-09	Rayment, Stephen G. et al.	
178	7546460		2009-06-09	Maes, Stephane H.	
179	7546629		2009-06-09	ALBERT, Anthony et al.	
180	7548875	B2	2009-06-16	Mikkelsen et al.	
181	7548976	B2	2009-06-16	Bahl, Paramvir et al.	
182	7551921	B2	2009-06-23	Petermann	
183	7551922		2009-06-23	Roskowski, Steve et al.	
184	7554983	B1	2009-06-30	Muppala, Suresh	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	185	7555757	B2	2009-06-30	Smith et al.	
	186	7561899	B2	2009-07-14	Lee, Changseok	
	187	7562213	B1	2009-07-14	Timms, Natalie	
	188	7564799	B2	2009-07-21	Holland et al.	
	189	7565141		2009-07-21	Macaluso, Anthony G.	
	190	7574509	B2	2009-08-11	Nixon et al.	
	191	7574731		2009-08-11	FASCENDA, Anthony C.	
	192	7577431	B2	2009-08-18	Jiang, Yue Jun	
	193	7580356	B1	2009-08-25	Mishra et al.	
	194	7580857		2009-08-25	VanFLEET et al.	
	195	7583964	B2	2009-09-01	Wong, Gregory A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	196	7584298	B2	2009-09-01	Klinker et al.	
	197	7586871	B2	2009-09-08	Hamilton et al.	
	198	7593417		2009-09-22	Wang, James et al.	
	199	7593730	B2	2009-09-22	Khandelwal, Deepak et al.	
	200	7596373	B2	2009-09-29	Mcgregor, Christopher et al.	
	201	7599288		2009-10-06	COLE, Raymond E. et al.	
	202	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	
	203	7602746	B2	2009-10-13	Calhoun et al.	
	204	7606918	B2	2009-10-20	Holzman et al.	
	205	7607041	B2	2009-10-20	Kraemer et al.	
	206	7609650		2009-10-27	ROSKOWSKI, Steve et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	207	7609700		2009-10-27	Ying, Wen-Ping et al.	
	208	7610047	B2	2009-10-27	Hicks III et al.	
	209	7610057	B2	2009-10-27	Bahl et al.	
	210	7610328		2009-10-27	HAASE et al.	
	211	7610396	B2	2009-10-27	Taglienti et al.	
	212	7614051	B	2009-11-03	Glaum et al.	
	213	7616962	B2	2009-11-10	Oswal, Anand K. et al.	
	214	7617516		2009-11-10	HUSLAK et al.	
	215	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	216	7620065		2009-11-17	FALARDEAU, Eric	
	217	7620162		2009-11-17	AARON et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

218	7620383	B2	2009-11-17	Taglienti et al.	
219	7627314		2009-12-01	Carlson, Steven I. et al.	
220	7627600	B2	2009-12-01	Citron et al.	
221	7627767	B2	2009-12-01	Sherman et al.	
222	7627872	B2	2009-12-01	Hebeier et al.	
223	7633438		2009-12-15	Tysowski, Piotr Konrad	
224	7634388		2009-12-15	Archer, Charles J. et al.	Entire Document
225	7636574		2009-12-22	Poosala, Viswanath	
226	7636626	B2	2009-12-22	Oesterling et al.	
227	7643411	B2	2010-01-05	Andreasen et al.	
228	7644151		2010-01-05	JERRIM, John et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

229	7644267		2010-01-05	YLIKOSKI, Martti et al.	
230	7644414	B2	2010-01-05	Smith et al.	
231	7647047		2010-01-12	MOGHADDAM et al.	
232	7650137		2010-01-19	JOBS et al.	
233	7653394	B2	2010-01-26	McMillin, Brian K.	
234	7656271	B2	2010-02-02	Ehrman et al.	
235	7657920	B2	2010-02-02	Arseneau et al.	
236	7660419	B1	2010-02-09	Ho, Jin-Meng	
237	7661124	B2	2010-02-09	Ramanathan et al.	
238	7664494	B2	2010-02-16	Jiang, Yue Jun	
239	7668176		2010-02-23	Chuah, Mooi Choo	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

240	7668612	B	2010-02-23	Okkonen, Harri	
241	7668903		2010-02-23	EDWARDS et al.	
242	7668966	B2	2010-02-23	Klinker et al.	
243	7676673	B2	2010-03-09	Weller et al.	
244	7680086	B2	2010-03-16	Eglin	
245	7681226	B2	2010-03-16	Kraemer et al.	
246	7684370	B2	2010-03-23	Kezys, Vytautas Robertas	
247	7685131		2010-03-23	Batra, Vishal Singh et al.	
248	7685254		2010-03-23	Pandya, Ashish A.	
249	7685530	B2	2010-03-23	Sherrard et al.	
250	7688792	B2	2010-03-30	Babbar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	251	7693107	B2	2010-04-06	De Froment, Eric	
	252	7693720		2010-04-06	KENNEWICK et al.	
	253	7697540	B2	2010-04-13	Haddad et al.	
	254	7707320	B2	2010-04-27	Singhai et al.	
	255	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	
	256	7711848		2010-05-04	MAES, Stephane H.	
	257	7719966	B2	2010-05-18	Luft et al.	
	258	7720206	B2	2010-05-18	Devolites et al.	
	259	7720464	B2	2010-05-18	Batta, Puneet	
	260	7720505		2010-05-18	GOPI et al.	
	261	7720960	B2	2010-05-18	Pruss, Richard Manfred et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	262	7721296	B2	2010-05-18	Ricagni, Giuseppe	
	263	7724716	B2	2010-05-25	Fadell, Anthony M.	
	264	7725570		2010-05-25	Lewis, Lundy	
	265	7729326		2010-06-01	Sekhar, Ramesh	
	266	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	267	7734784		2010-06-08	ARAUJO et al.	
	268	7742406	B1	2010-06-22	Muppala, Suresh	
	269	7746854		2010-06-29	AMBE, Shekhar et al.	
	270	7747240		2010-06-29	BRISCOE et al.	
	271	7747699		2010-06-29	PRUEITT et al.	
	272	7747730		2010-06-29	HARLOW, James D.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

273	7752330	B2	2010-07-06	Olsen et al.	
274	7756056	B2	2010-07-13	Kim et al.	
275	7756534		2010-07-13	Anupam, Vinod et al.	
276	7756757	B1	2010-07-13	Oakes III, Charles Lee	
277	7760137	B2	2010-07-20	Martucci et al.	
278	7760711	B1	2010-07-20	Kung et al.	
279	7760861		2010-07-20	Croak, Marian et al.	
280	7765294	B2	2010-07-27	Edwards et al.	
281	7769397	B2	2010-08-03	Funato et al.	
282	7770785	B2	2010-08-10	Jha et al.	
283	7774323	B2	2010-08-10	Helfman, Nadav	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	284	7774412	B1	2010-08-10	Schnepel, Soenke	
	285	7774456	B1	2010-08-10	Lownsborough, Derek Leigh et al.	
	286	7778176		2010-08-17	Morford, Michael Robert	
	287	7778643		2010-08-17	Laroia, Rajiv et al.	
	288	7792257	B1	2010-09-07	Vanier et al.	
	289	7792538		2010-09-07	Kozisek, Steven E.	
	290	7792708		2010-09-07	ALVA, Jessi	
	291	7797019	B2	2010-09-14	Friedmann	
	292	7797060	B2	2010-09-14	Grgic et al.	
	293	7797204		2010-09-14	BALENT, Bruce F.	
	294	7797401		2010-09-14	STEWART et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	295	7801523		2010-09-21	Kenderov, Stoyan	
	296	7801783	B2	2010-09-21	Kende et al.	
	297	7801985	B1	2010-09-21	Pitkow, Jim et al.	
	298	7802724		2010-09-28	Nohr, Steven Paul	
	299	7805140	B2	2010-09-28	Friday et al.	
	300	7805522	B2	2010-09-28	Schlüter et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	1							☐
--	---	--	--	--	--	--	--	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237
	Filing Date		2022-01-17
	First Named Inventor	RALEIGH, GREGORY	
	Art Unit	2414	
	Examiner Name	NOT YET ASSIGNED	
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	7805606	B2	2010-09-28	Birger et al.	
	2	7809351	B1	2010-10-05	Panda et al.	
	3	7809372	B2	2010-10-05	Rajaniemi, Jaakko	
	4	7813746	B2	2010-10-12	Rajkotia, Purva R.	
	5	7817615	B1	2010-10-19	Breau et al.	
	6	7817983	B2	2010-10-19	Cassett et al.	
	7	7822837		2010-10-26	URBAN et al.	
	8	7822849	B2	2010-10-26	Titus	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

9	7826427	B2	2010-11-02	Sood et al.	
10	7826607	B1	2010-11-02	De Carvalho Resende et al.	
11	7835275	B1	2010-11-16	Swan et al.	
12	7843831	B2	2010-11-30	Morrill et al.	
13	7843843	B1	2010-11-30	Papp III et al.	
14	7844034	B1	2010-11-30	Oh et al.	
15	7844728	B2	2010-11-30	Anderson et al.	
16	7848768		2010-12-07	OMORI et al.	
17	7849161	B2	2010-12-07	Koch et al.	
18	7849170	B1	2010-12-07	Hargens et al.	
19	7849477	B2	2010-12-07	Cristofalo et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

20	7853255	B2	2010-12-14	Karaoguz et al.	
21	7853656	B2	2010-12-14	Yach et al.	
22	7856226		2010-12-21	WONG, Ellis L. et al.	
23	7860088	B2	2010-12-28	Lioy, Marcello	
24	7865182		2011-01-04	Macaluso, Anthony G.	
25	7865187	B2	2011-01-04	Ramer et al.	
26	7868778		2011-01-11	KENWRIGHT, David Norris	
27	7873001	B2	2011-01-18	Silver, Andrew	
28	7873344		2011-01-18	BOWSER, Robert et al.	
29	7873346	B2	2011-01-18	Petersson et al.	
30	7873540	B2	2011-01-18	Arumugam, Avin	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	31	7873705		2011-01-18	KALISH, Dan	
	32	7877090		2011-01-25	Maes, Stephane H.	
	33	7881199		2011-02-01	KRSTULICH, Zlatko	
	34	7881697	B2	2011-02-01	Baker, Matthew Donald et al.	
	35	7882029		2011-02-01	WHITE, Craig R.	
	36	7882247	B2	2011-02-01	Stumolo et al.	
	37	7882560	B2	2011-02-01	Kraemer et al.	
	38	7885644	B2	2011-02-08	Gallagher et al.	
	39	7886047		2011-02-08	POTLURI, Dora	
	40	7889384	B2	2011-02-15	Armentrout et al.	
	41	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	7890111		2011-02-15	Bugenhagen, Michael K.	
43	7894431	B2	2011-02-22	Goring et al.	
44	7899039	B2	2011-03-01	Andreasen et al.	
45	7899438	B2	2011-03-01	Baker, Matthew Donald et al.	
46	7903553		2011-03-08	Liu, Enhui	
47	7907970		2011-03-15	Park, Vincent D. et al.	
48	7911975		2011-03-22	DROZ, Patrick et al.	
49	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
50	7912056		2011-03-22	BRASSEM, Wayne	
51	7920529		2011-04-05	MAHLER, Roger et al.	
52	7921463		2011-04-05	Sood, Kapil et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	7925740	B2	2011-04-12	Nath et al.	
54	7925778	B1	2011-04-12	Wijnands et al.	
55	7929446	B2	2011-04-19	Bozarth et al.	
56	7929959	B2	2011-04-19	DeAtley, Dallas et al.	
57	7929960		2011-04-19	MARTIN et al.	
58	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
59	7930327	B2	2011-04-19	Craft David et al.	
60	7930446	B2	2011-04-19	Kesselman, Alex et al.	
61	7930553	B2	2011-04-19	Satarasinghe et al.	
62	7933274	B2	2011-04-26	Verma et al.	
63	7936736	B2	2011-05-03	Proctor Jr. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

64	7937069		2011-05-03	RASSAM, Frederic	
65	7937450	B2	2011-05-03	Janik, Craig M.	
66	7940685	B1	2011-05-10	Breslau, Lee et al.	
67	7940751		2011-05-10	Hansen, Christopher J.	
68	7941184		2011-05-10	PRENDERGAST et al.	
69	7944948		2011-05-17	Chow, Albert T. et al.	
70	7945238	B2	2011-05-17	Baker, Matthew Donald et al.	
71	7945240		2011-05-17	KLOCK, Jacqueline et al.	
72	7945945		2011-05-17	Graham, Richard et al.	
73	7948952		2011-05-24	HURTTA, Tuija et al.	
74	7948953	B2	2011-05-24	Melkote, Keerti G. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	75	7948968		2011-05-24	Voit, Eric A. et al.	
	76	7949529		2011-05-24	WEIDER et al.	
	77	7953808		2011-05-31	SHARP et al.	
	78	7953877	B2	2011-05-31	Vemula et al.	
	79	7957020		2011-06-07	MINE, Ryuta et al.	
	80	7957381	B2	2011-06-07	Clermidy et al.	
	81	7957511		2011-06-07	DRUDIS et al.	
	82	7958029	B1	2011-06-07	Bobich et al.	
	83	7962622		2011-06-14	Friend, John et al.	
	84	7965983		2011-06-21	SWAN, Tim et al.	
	85	7966405	B2	2011-06-21	Sundaresan et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

86	7969950	B2	2011-06-28	Iyer et al.	
87	7970350		2011-06-28	SHEYNMAN, Arnold	
88	7970426		2011-06-28	Poe, Brian R. et al.	
89	7974624		2011-07-05	Gallagher, Michael D. et al.	
90	7975184		2011-07-05	GOFF et al.	
91	7978627		2011-07-12	TAYLOR, William Scott et al.	
92	7978686	B2	2011-07-12	Goyal et al.	
93	7979069	B2	2011-07-12	Hupp et al.	
94	7979889	B2	2011-07-12	Gladstone et al.	
95	7979896	B2	2011-07-12	McMurtry et al.	
96	7984130		2011-07-19	BOGINENI et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

97	7984511	B2	2011-07-19	Kocher Paul et al.	
98	7986935		2011-07-26	D'SOUZA et al.	
99	7987496	B2	2011-07-26	Bryce et al.	
100	7987510	B2	2011-07-26	Kocher et al.	
101	7990049	B2	2011-08-02	Shioya, Shunsuke	
102	8000276	B2	2011-08-16	Scherzer, Shimon et al.	
103	8000318		2011-08-16	Wiley, William L. et al.	
104	8005009		2011-08-23	McKee, Neil et al.	
105	8005459		2011-08-23	BALSILLIE, Jim	
106	8005726	B1	2011-08-23	Bao, Yulin	
107	8005913	B1	2011-08-23	Carlander, Carrie	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	108	8005988		2011-08-23	MAES, Stephane H.	
	109	8010080		2011-08-30	THENTHIRUPERAI et al.	
	110	8010081		2011-08-30	ROSKOWSKI, Steve	
	111	8010082	B2	2011-08-30	Sutaria et al.	
	112	8010990	B2	2011-08-30	Ferguson et al.	
	113	8015133		2011-09-06	WU et al.	
	114	8015234		2011-09-06	LUM et al.	
	115	8015249	B2	2011-09-06	Nayak et al.	
	116	8019687		2011-09-13	WANG et al.	
	117	8019820		2011-09-13	Son, Giyeong et al.	
	118	8019846	B2	2011-09-13	Roelens et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	119	8019868		2011-09-13	RAO, Goutham et al.	
	120	8023425	B2	2011-09-20	Raleigh	
	121	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	122	8024424	B2	2011-09-20	Freimuth et al.	
	123	8027339	B2	2011-09-27	Short, Joel E. et al.	
	124	8031601	B2	2011-10-04	Feroz et al.	
	125	8032168	B2	2011-10-04	Ikaheimo, Jorma	
	126	8032409	B1	2011-10-04	Mikurak	
	127	8032899	B2	2011-10-04	Archer, Charles J. et al.	
	128	8036387	B2	2011-10-11	Kudelski et al.	
	129	8044792	B2	2011-10-25	Orr et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

130	8045973	B2	2011-10-25	Chambers, Michael D.	
131	8046449	B2	2011-10-25	Yoshiuchi, Hideya	
132	8050275		2011-11-01	IYER, Jayaraman R.	
133	8050690	B2	2011-11-01	Neeraj, Chawla	
134	8050705	B2	2011-11-01	Sicher et al.	
135	8059530		2011-11-15	Cole, Terry L.	
136	8060017	B2	2011-11-15	Schlicht et al.	
137	8060463		2011-11-15	Spiegel, Joel R.	
138	8064418	B2	2011-11-22	Maki, Lasse	
139	8065365	B2	2011-11-22	Saxena et al.	
140	8068824		2011-11-29	SHAN, Xueshan et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

141	8068829	B2	2011-11-29	Lemond, Eric et al.	
142	8073427	B2	2011-12-06	Koch et al.	
143	8073721		2011-12-06	Lewis, Lundy	
144	8078140	B2	2011-12-13	Baker, Matthew Donald et al.	
145	8078163	B2	2011-12-13	Lemond, Eric et al.	
146	8085808	B2	2011-12-27	Brusca et al.	
147	8086398	B2	2011-12-27	Sanchez et al.	
148	8086497	B1	2011-12-27	Oakes III, Charles Lee	
149	8086791	B2	2011-12-27	Caulkins, Jason	
150	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
151	8090361	B2	2012-01-03	Hagan, Guy R.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	152	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	153	8091087	B2	2012-01-03	Ali et al.	
	154	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	155	8095112	B2	2012-01-10	Chow, Richard et al.	
	156	8095640	B2	2012-01-10	Guingo et al.	
	157	8095666		2012-01-10	SCHMIDT et al.	
	158	8098579		2012-01-17	Ray, Amar N. et al.	
	159	8099077		2012-01-17	CHOWDHURY et al.	
	160	8099517		2012-01-17	JIA et al.	
	161	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	162	8103285	B2	2012-01-24	Kaihan, Amit	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	163	8104080	B2	2012-01-24	Burns et al.	
	164	8107953	B2	2012-01-31	Zimmerman et al.	
	165	8108520		2012-01-31	Ruutu, Jussi et al.	
	166	8108680	B2	2012-01-31	Murray	
	167	8112435	B2	2012-02-07	Epstein et al.	
	168	8116223		2012-02-14	TIAN, Dan et al.	
	169	8116749		2012-02-14	Proctor Jr., James Arthur et al.	
	170	8116781	B2	2012-02-14	Chen, Xixian et al.	
	171	8122128		2012-02-21	Burke, II, Robert M. et al.	
	172	8122249		2012-02-21	Falk, Rainer et al.	
	173	8125897	B2	2012-02-28	Ray et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	174	8126123		2012-02-28	Cai, Yigang et al.	
	175	8126396	B2	2012-02-28	Bennett, James D.	
	176	8126476	B2	2012-02-28	Vardi, Yosef et al.	
	177	8126722		2010-02-28	ROBB, Terence Alan et al.	
	178	8130793	B2	2012-03-06	Edwards, Stephen K. et al.	
	179	8131256		2012-03-06	MARTTI, Jyrki et al.	
	180	8131281	B1	2012-03-06	Hildner et al.	
	181	8131840	B1	2012-03-06	Denker, Richard E.	
	182	8131858	B2	2012-03-06	Agulnik et al.	
	183	8132256	B2	2012-03-06	Bari, Farooq	
	184	8134954	B2	2012-03-13	Godfrey, James A. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

185	8135388		2012-03-13	Gailloux, Michael A. et al.	
186	8135392		2012-03-13	MARCELLINO et al.	
187	8135657		2012-03-13	Kapoor, Harsh et al.	
188	8140690	B2	2012-03-20	Ly et al.	
189	8144591		2012-03-27	GHAJ et al.	
190	8145194	B2	2012-03-27	Yoshikawa et al.	
191	8146142	B2	2012-03-27	Lortz et al.	
192	8149748	B2	2012-04-03	Bata et al.	
193	8149823		2012-04-03	Turcan, Diane Brown et al.	
194	8150394	B2	2012-04-03	Bianconi et al.	
195	8150431		2012-04-03	Wolovitz, Lionel et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

196	8151205	B2	2012-04-03	Follmann et al.	
197	8155155		2012-04-10	Chow, Albert T. et al.	
198	8155620		2012-04-10	Wang, Jun et al.	
199	8155666	B2	2012-04-10	Alizadeh-Shabdiz, Farshid	
200	8155670		2012-04-10	Fullam, Scott et al.	
201	8156206		2012-04-10	KILEY, Kevin J. et al.	
202	8159520	B1	2012-04-17	Dhanoa et al.	
203	8160056	B2	2012-04-17	Van der Merwe et al.	
204	8160598	B2	2012-04-17	Savoor, Raghvendra	
205	8165576		2012-04-24	Raju, Vishwanath et al.	
206	8166040	B2	2012-04-24	Brindisi, Richard G. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

207	8166554	B2	2012-04-24	John, Pramod	
208	8170553		2012-05-01	BENNETT, James D.	
209	8174378	B2	2012-05-08	Richman et al.	
210	8174970	B2	2012-05-12	Adamczyk, Maria et al.	
211	8175574	B1	2012-05-08	Panda et al.	
212	8180881	B2	2012-05-15	Seo et al.	
213	8180886	B2	2012-05-15	Overcash et al.	
214	8184530		2012-05-22	SWAN, Tim L. et al.	
215	8184590		2012-05-22	Rosenblatt, Ariel	
216	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
217	8185127	B1	2012-05-22	Cai et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	218	8185152		2012-05-22	GOLDNER, Alla	
	219	8185158		2012-05-22	Tamura, Motoshi et al.	
	220	8190087	B2	2012-05-29	Fisher et al.	
	221	8190122	B1	2012-05-29	Alexander et al.	
	222	8190675		2012-05-29	TRIBBETT, David	
	223	8191106	B2	2012-05-29	Choyi et al.	
	224	8191116		2012-05-29	Gazzard, Daryl	
	225	8191124	B2	2012-05-29	Wynn et al.	
	226	8194549	B2	2012-06-05	Huber et al.	
	227	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	228	8194581	B1	2012-06-05	Schroeder et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	229	8195153	B1	2012-06-05	Frencel et al.	
	230	8195163	B2	2012-06-05	Gisby, Doug et al.	
	231	8195661	B2	2012-06-05	Kalavade, Asawaree	
	232	8196199	B2	2012-06-05	Hrastar et al.	
	233	8200163	B2	2012-06-12	Hoffman, George E.	
	234	8200200	B1	2012-06-12	Beiser et al.	
	235	8200509	B2	2012-06-12	Kenedy, Andrew Alexander et al.	
	236	8200775		2012-06-12	MOORE, James F.	
	237	8200818	B2	2012-06-12	Freund et al.	
	238	8204190	B2	2012-06-19	Bang et al.	
	239	8204505	B2	2012-06-19	Jin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	240	8208788	B2	2012-06-26	Ando et al.	
	241	8208919		2012-06-26	KOTECHEA, Lalit Ratilal	
	242	8213296		2012-07-03	SHANNON, Frank M. et al.	
	243	8213363		2012-07-03	Ying, Wen-Ping et al.	
	244	8214536		2012-07-03	ZHAO, Wen	
	245	8214890	B2	2012-07-03	Kirovski et al.	
	246	8219134	B2	2012-07-10	Maharajh et al.	
	247	8223655	B2	2012-07-17	Heinz et al.	
	248	8224382		2012-07-17	Bultman, Michael J.	
	249	8224773		2012-07-17	Spiegel, Joel R.	
	250	8228818	B2	2012-07-24	Chase et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	251	8229394	B2	2012-07-24	Karlberg, Johan	
	252	8229914	B2	2012-07-24	Ramer et al.	
	253	8233433	B2	2012-07-31	Kalhan, Amit	
	254	8233883		2012-07-31	De Froment, Eric	
	255	8233895		2012-07-31	Tysowski, Piotr Konrad	
	256	8238287		2012-08-07	Gopi, Paramesh et al.	
	257	8239520		2012-08-07	GRAH, Adrian	
	258	8242959	B2	2012-08-14	Mia, Rashidus S. et al.	
	259	8244241		2012-08-14	Montemurro, Michael	
	260	8249601	B2	2012-08-21	Emberson et al.	
	261	8254880	B2	2012-08-28	Aaltonen et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	262	8254915		2012-08-28	Kozisek, Steven E.	
	263	8255515		2012-08-28	MELMAN, David et al.	
	264	8255534	B2	2012-08-28	Assadzadeh, Alireza	
	265	8255689		2012-08-28	KIM, Eun Ah et al.	
	266	8259692	B2	2012-09-04	Bajko, Gabor	
	267	8264965	B2	2012-09-11	Dolganow et al.	
	268	8265004		2012-09-11	Toutonghi, Michael J.	
	269	8266249	B2	2012-09-11	Hu	
	270	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	271	8270955	B2	2012-09-18	Ramer et al.	
	272	8270972	B2	2012-09-18	Otting, Marcia J. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

273	8271025	B2	2012-09-18	Brisebois et al.	
274	8271045		2012-09-18	Parolkar, Satish et al.	
275	8271049		2012-09-18	SILVER, Andrew et al.	
276	8271992	B2	2012-09-18	Chatley, Scott P. et al.	
277	8275415	B2	2012-09-25	Huslak, Nicholas S.	
278	8279067		2012-10-02	BERGER, Thomas R. et al.	
279	8279864		2012-10-02	Wood, Daniel M.	
280	8280354		2012-10-02	Smith, Christopher et al.	
281	8284740		2012-10-09	O'CONNOR, Dennis M.	
282	8285249	B2	2012-10-09	Baker, Matthew Donald et al.	
283	8285992	B2	2012-10-09	Mathur et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

284	8291238		2012-10-16	GINTER, Karl L. et al.	
285	8291439	B2	2012-10-16	Jethi et al.	
286	8296404		2012-10-23	McDysan, Dave et al.	
287	8300575	B2	2012-10-30	Willars, Per	
288	8307067	B2	2012-11-06	Ryan, Nicholas M.	
289	8310943	B2	2012-11-13	Mehta et al.	
290	8315198	B2	2012-11-20	Corneille et al.	
291	8315593	B2	2012-11-20	Gallant et al.	
292	8315999	B2	2012-11-20	Chatley, Scott P. et al.	
293	8320244	B2	2012-11-27	Muqattash et al.	
294	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	295	8325638		2012-12-04	Jin, Haipeng et al.	
	296	8325906	B2	2012-12-04	Fullarton et al.	
	297	8326319	B2	2012-12-04	Davis, Richard W.	
	298	8326828	B2	2012-12-04	Zhou et al.	
	299	8331223	B2	2012-12-11	Hill et al.	
	300	8331293		2012-12-11	Sood, Kapil	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	1							☐
--	---	--	--	--	--	--	--	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-22)

Approved for use through 05/31/2024. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17577237
	Filing Date	2022-01-17
	First Named Inventor	RALEIGH, GREGORY
	Art Unit	2414
	Examiner Name	NOT YET ASSIGNED
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	8332375		2012-12-11	Chatley, Scott P. et al.	
	2	8339991	B2	2012-12-25	Biswas et al.	
	3	8340625	B1	2012-12-25	Johnson et al.	
	4	8340678	B1	2012-12-25	Pandey, Vinod	
	5	8340718		2012-12-25	Colonna, Massimo et al.	
	6	8346210	B2	2013-01-01	Balsan et al.	
	7	8346923	B2	2013-01-01	Rowles et al.	
	8	8347104	B2	2013-01-01	Pathiyai, Krishna K.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

9	8347378	B2	2013-01-01	Merkin et al.	
10	8350700		2013-01-08	Fast, Raymond D. et al.	
11	8351592	B2	2013-01-08	Freeny Jr et al.	
12	8351898	B2	2013-01-08	Raleigh	
13	8352360	B2	2013-01-08	De Judicibus et al.	
14	8352980		2013-01-08	Howcroft, Jerald Robert	
15	8355696	B1	2013-01-15	Olding et al.	
16	8356336	B2	2013-01-15	Johnston, Keith et al.	
17	8358638	B2	2013-01-22	Scherzer, Tamir et al.	
18	8358975	B2	2013-01-22	Bahl et al.	
19	8363658		2013-01-29	Delker, Jason R. et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

20	8363799	B2	2013-01-29	Gruchala et al.	
21	8364806		2013-01-29	Short, Joel E. et al.	
22	8370477		2013-02-05	Short, Joel E. et al.	
23	8370483	B	2013-02-05	Choong Jason et al.	
24	8374090		2013-02-12	Morrill, Robert J. et al.	
25	8374592		2013-02-12	Proctor, Jr. James A. et al.	
26	8375128	B2	2013-02-12	Tofighbakhsh et al.	
27	8375136	B2	2013-02-12	Roman et al.	
28	8380247	B2	2013-02-19	Engstrom	
29	8385199	B1	2013-02-26	Coward et al.	
30	8385896		2013-02-26	Proctor Jr., James A. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	31	8385964	B2	2013-02-26	Haney, Richard D.	
	32	8386386		2013-02-26	Zhu, Kevin	
	33	8392982	B2	2013-03-05	Harris et al.	
	34	8396929		2013-03-12	Helfman, Nadav et al.	
	35	8401906	B2	2013-03-19	Ruckart	
	36	8401968	B1	2013-03-19	Schattauer et al.	
	37	8402165	B2	2013-03-19	Deu-Ngoc et al.	
	38	8402540		2013-03-19	Kapoor, Harsh et al.	
	39	8406736	B2	2013-03-26	Das et al.	
	40	8407763	B2	2013-03-26	Weller et al.	
	41	8411587		2013-04-02	Curtis, William et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

42	8411691	B2	2013-04-02	Aggarwal	
43	8413245	B2	2013-04-02	Kraemer et al.	
44	8418168	B2	2013-04-09	Tyhurst et al.	
45	8423016		2013-04-16	BUCKLEY, Adrian et al.	
46	8429403		2013-04-23	Moret, Eric et al.	
47	8437734		2013-05-07	Ray, Amar N. et al.	
48	8442015	B2	2013-05-14	Behzad et al.	
49	8446831	B2	2013-05-21	Kwan et al.	
50	8447607	B2	2013-05-21	Weider, Chris et al.	
51	8447980		2013-05-21	Godfrey, James A. et al.	
52	8448015	B2	2013-05-21	Gerhart, David	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

53	8461958	B2	2013-06-11	Saenz et al.	
54	8463194	B2	2013-06-11	Erlenback et al.	
55	8463232	B2	2013-06-11	Tuli et al.	
56	8468337	B2	2013-06-18	Gaur, Santosh P. et al.	
57	8472371		2013-06-25	Bari, Farooq et al.	
58	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
59	8483135		2013-07-09	Cai, Yigang et al.	
60	8483694	B2	2013-07-09	Lewis et al.	
61	8484327	B2	2013-07-09	Werner et al.	
62	8488597	B2	2013-07-16	Nie et al.	
63	8489110	B2	2013-07-16	Frank et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

64	8489720	B1	2013-07-16	Morford, Michael et al.	
65	8494559	B1	2013-07-23	Malmi	
66	8495181	B2	2013-07-23	Venkatraman et al.	
67	8495227		2013-07-23	Kaminsky, David L. et al.	
68	8495360		2013-07-23	Falk, Rainer et al.	
69	8495700	B2	2013-07-23	Shahbazi	
70	8495743	B2	2013-07-23	Kraemer et al.	
71	8500533	B2	2013-08-06	Lutnick et al.	
72	8503358	B2	2013-08-06	Hanson et al.	
73	8503455	B2	2013-08-06	Heikens, Heico	
74	8504032	B2	2013-08-06	Lott et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

75	8504574	B2	2013-08-06	Dvorak et al.	
76	8504687	B2	2013-08-06	Maffione et al.	
77	8504729		2013-08-06	Pezzutti, David A.	
78	8505073	B2	2013-08-06	Taglienti et al.	
79	8509082	B2	2013-08-13	Heinz, John M. et al.	
80	8514927	B2	2013-08-20	Sundararajan et al.	
81	8520589		2013-08-27	Bhatt, Yogesh et al.	
82	8521110		2013-08-27	Rofougaran, Ahmadreza	
83	8521775	B1	2013-08-27	Poh et al.	
84	8522039	B2	2013-08-27	Hyndman et al.	
85	8522249	B2	2013-08-27	Beaule, Stephane	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

86	8522337	B2	2013-08-27	Adusumilli et al.	
87	8523547	B2	2013-09-03	Pekrul, Merton W.	
88	8526329	B2	2013-09-03	Mahany, Ronald L. et al.	
89	8526350	B2	2013-09-03	Xue, Qi et al.	
90	8527410	B2	2013-09-03	Markki et al.	
91	8527662	B2	2013-09-03	Biswas et al.	
92	8528068	B1	2013-09-03	Weglein et al.	
93	8531954	B2	2013-09-10	McNaughton et al.	
94	8531995	B2	2013-09-10	Khan et al.	
95	8532610	B2	2013-09-10	Manning Cassett et al.	
96	8533775	B2	2013-09-10	Alcorn et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

97	8535160	B2	2013-09-17	Lutnick et al.	
98	8538394	B2	2013-09-17	Zimmerman et al.	
99	8538421	B2	2013-09-17	Brisebois et al.	
100	8538458	B2	2013-09-17	Haney, Richard D.	
101	8539544	B2	2013-09-17	Garimella et al.	
102	8543265	B2	2013-09-24	Ekhuagere et al.	
103	8543814	B2	2013-09-24	Laitinen et al.	
104	8544105	B2	2013-09-24	McLean et al.	
105	8548427	B2	2013-10-01	Chow et al.	
106	8554876	B2	2013-10-08	Winsor, Gerald W.	
107	8559369	B2	2013-10-15	Barkan	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	108	8561138	B2	2013-10-15	Rothman, Michael M. et al.	
	109	8565746	B2	2013-10-22	Hoffman, George E.	
	110	8566236	B2	2013-10-22	Busch, James David	
	111	8571474	B2	2013-10-29	Chavez et al.	
	112	8571501	B2	2013-10-29	Miller et al.	
	113	8571598	B2	2013-10-29	Vaiavi, John J.	
	114	8571993	B2	2013-10-29	Kocher et al.	
	115	8572117	B2	2013-10-29	Rappaport, Theodore S.	
	116	8572256	B2	2013-10-29	Babbar, Uppinder Singh	
	117	8583499		2013-11-12	De Judicibus, Dario et al.	
	118	8588240	B2	2013-11-19	Ramankutty et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

119	8589955	B2	2013-11-19	Roundtree et al.	
120	8594665	B2	2013-11-26	Anschutz, Thomas	
121	8595186	B1	2013-11-26	Mandyam et al.	
122	8600895	B2	2013-12-03	Felsher, David Paul	
123	8601125	B2	2013-12-03	Huang et al.	
124	8605691	B2	2013-12-10	Soomro et al.	
125	8611919	B2	2013-12-17	Barnes Jr.	
126	8615507	B2	2013-12-24	VARADARAJULU et al.	
127	8620257	B2	2013-12-31	Qiu et al.	
128	8634425	B2	2014-01-21	Gorti et al.	
129	8635164	B2	2014-01-21	Rosenhaft et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

130	8639215	B2	2014-01-28	McGregor et al.	
131	8644702	B1	2014-02-04	Kalajan, Kevin E.	
132	8644813	B1	2014-02-04	Gailloux et al.	
133	8645518	B	2014-02-04	David, Scott L.	
134	8655357	B1	2014-02-18	Gazzard et al.	
135	8656472	B2	2014-02-18	McMurtry et al.	
136	8660853	B2	2014-02-25	Robb et al.	
137	8666395	B2	2014-03-04	Silver, Andrew	
138	8667542	B1	2014-03-04	Bertz et al.	
139	8670334	B	2014-03-11	Keohane et al.	
140	8675852	B2	2014-03-18	Maes, Stephane H.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

141	8676682	B2	2014-03-18	Kalliola, Janne	
142	8676925	B	2014-03-18	Liu et al.	
143	8693323		2014-04-08	McDysan, David E.	
144	8694772	B2	2014-04-08	Kao et al.	
145	8700729	B2	2014-04-15	Dua, Robin	
146	8701015	B2	2014-04-15	Bonnat, Pierre	
147	8706863		2014-04-22	Fadell, Anthony	
148	8713535	B2	2014-04-29	Malhotra et al.	
149	8713641	B1	2014-04-29	Pagan et al.	
150	8719397	B2	2014-05-06	Levi et al.	
151	8719423	B2	2014-05-06	Wyld	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

152	8725899	B	2014-05-13	Short et al.	
153	8730842	B2	2014-05-20	Collins et al.	
154	8731519	B2	2014-05-20	Flynn et al.	
155	8732808	B2	2014-05-20	Sewall et al.	
156	8739035	B2	2014-05-27	Trethewey, Jim	
157	8744339	B2	2014-06-03	Halfmann et al.	
158	8761711	B2	2014-06-24	Grignani et al.	
159	8761809	B2	2014-06-24	Faith et al.	
160	8780857	B2	2014-07-15	Balasubramanian et al.	
161	8787249	B2	2014-07-22	Giaretta et al.	
162	8793304	B2	2014-07-29	Lu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor	RALEIGH, GREGORY		
	Art Unit	2414		
	Examiner Name	NOT YET ASSIGNED		
	Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1		

	163	8798610	B2	2014-08-05	Prakash et al.	
	164	8804695	B2	2014-08-12	Branam	
	165	8811338	B2	2014-08-19	Jin et al.	
	166	8811991	B2	2014-08-19	Jain et al.	
	167	8818394	B2	2014-08-26	Bienas et al.	
	168	8819253	B2	2014-08-26	Simeloff et al.	
	169	8825109	B2	2014-09-02	Montemurro et al.	
	170	8826411	B2	2014-09-02	Moen et al.	
	171	8831561	B2	2014-09-09	Sutaria et al.	
	172	8838752	B2	2014-09-16	Lor et al.	
	173	8845415	B2	2014-09-30	Lutnick et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

174	8849297	B2	2014-09-30	Balasubramanian	
175	8855620	B2	2014-10-07	Sievers et al.	
176	8862751	B2	2014-10-14	Faccin et al.	
177	8875042	B2	2014-10-28	LeJeune et al.	
178	8880047	B2	2014-11-04	Konicek et al.	
179	8908516	B2	2014-12-09	Tzamaloukas et al.	
180	8929374	B2	2015-01-06	Tönsing et al.	
181	8930238	B2	2015-01-06	Coffman et al.	
182	8943551	B2	2015-01-27	Ganapathy et al.	
183	8948726	B2	2015-02-03	Smith et al.	
184	8949382	B2	2015-02-03	Cornett et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

185	8955038	B2	2015-02-10	Nicodemus et al.	
186	8966018	B2	2015-02-24	Bugwadia et al.	
187	8971912	B2	2015-03-03	Chou et al.	
188	8977284	B2	2015-03-10	Reed, Mark J.	
189	8995952	B1	2015-03-31	Baker et al.	
190	9002342	B2	2015-04-07	Tenhunen et al.	
191	9014973	B2	2015-04-21	Ruckart, John	
192	9015331	B2	2015-04-21	Lai et al.	
193	9030934	B2	2015-05-12	Shah et al.	
194	9049010		2015-06-02	Jueneman et al.	
195	9064275	B1	2015-06-23	Lu et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

	196	9105031	B2	2015-08-11	Shen et al.	
	197	9111088	B2	2015-08-18	Ghai et al.	
	198	9137286	B1	2015-09-15	Yuan	
	199	9172553	B2	2015-10-27	Dawes et al.	
	200	9262370	B2	2016-02-16	Hofstaedter et al.	
	201	9286469	B2	2016-03-15	Kraemer et al.	
	202	9286604	B2	2016-03-15	Aabye et al.	
	203	9313708	B2	2016-04-12	Nam et al.	
	204	9325737	B2	2016-04-26	Gulowski et al.	
	205	9326173	B2	2016-04-26	Luft, Achim	
	206	9344557	B2	2016-05-17	Gruchala et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	207	9363285	B2	2016-06-07	Kitamura	
	208	9367680	B2	2016-06-14	Mahaffey et al.	
	209	9413546	B2	2016-08-09	Meier et al.	
	210	9418381	B2	2016-08-16	Ahuja et al.	
	211	9501803	B2	2016-11-22	Bilac et al.	
	212	9516456	B2	2016-12-06	Stephens et al.	
	213	9589117	B2	2017-03-07	Ali et al.	
	214	9615192	B2	2017-04-04	Raleigh	
	215	RE44412		2013-08-06	Naqvi et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
-------------------	---------	--------------------	------------------------	------------------	---	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17577237	
	Filing Date		2022-01-17	
	First Named Inventor		RALEIGH, GREGORY	
	Art Unit		2414	
	Examiner Name		NOT YET ASSIGNED	
	Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	

	1					
--	---	--	--	--	--	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	17577237
Filing Date	2022-01-17
First Named Inventor	RALEIGH, GREGORY
Art Unit	2414
Examiner Name	NOT YET ASSIGNED
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Farshad Farjami/	Date (YYYY-MM-DD)	2022-05-23
Name/Print	Farshad Farjami	Registration Number	41,014

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	45791098
Application Number:	17577237
International Application Number:	
Confirmation Number:	5850
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	Michael Farjami/Evan Gunderman
Filer Authorized By:	Michael Farjami
Attorney Docket Number:	RALEP007C11C3C2C3C2C1C1C1
Receipt Date:	24-MAY-2022
Filing Date:	17-JAN-2022
Time Stamp:	15:04:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		RALEP007C11C3C2C3C2C1C1C1_IDS_May_24_22.pdf	876828	yes	164
			e8899a0879ed3a077f994d62bdcc19e71adc05e2		

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Transmittal Letter	1	1
	Information Disclosure Statement (IDS) Form (SB08)	2	164
Warnings:			
Information:			
Total Files Size (in bytes):		876828	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>			



FARJAMI & FARJAMI LLP
AN INTELLECTUAL PROPERTY LAW FIRM

www.farjami.com

26522 La Alameda Avenue, Suite 360
Mission Viejo, California 92691
tel: (949) 282-1000
fax: (949) 282-1002

ELECTRONIC TRANSMISSION COVER SHEET

Date: May 24, 2022

To: United States Patent and Trademark Office
Examiner: Unknown; Art Unit: Unknown

Re: **Application Serial No.: 17/577,237**
Filing Date: 1/17/2022; First-Named Inventor: Raleigh
Attorney Docket No.: RALEP007C11C3C2C3C2C1C1C1

From: Farjami & Farjami LLP

Number of pages including the cover sheet: 164

Message:

Enclosed, please find the Information Disclosure Statement and Form PTO-1449.

Authorization is hereby given to the Commissioner to charge any fees associated with this communication or credit any overpayment to Deposit Account **50-0731**.

The documents accompanying this electronic transmission contain **PRIVILEGED AND CONFIDENTIAL** information intended only for use of the individual or entity named above. If you are not the intended recipient, disclosure, copying, distribution or use of the contents of this electronic transmission information is prohibited. If you have received this electronic transmission in error, please immediately notify us by telephone and return the original electronic transmission to us at the above address via U.S. Postal Service. We will reimburse you for all expenses incurred.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO.	TOT CLAIMS	IND CLAIMS
17/577,237	01/17/2022	2414	0.00	RALEP007C11C3C2C3C2C1C1C1	1	1

CONFIRMATION NO. 5850

FILING RECEIPT



0000000131387695

106963
Headwater Research LLC
110 North College Avenue
Suite 1116
Tyler, TX 75702

Date Mailed: 01/27/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Gregory G. Raleigh, Incline Village, NV;

Applicant(s)

Headwater Research LLC, Tyler, TX;

Assignment For Published Patent Application

Headwater Research LLC, Tyler, TX

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 16/436,628 06/10/2019 PAT 11228617
which is a CON of 15/582,350 04/28/2017 PAT 10321320
which is a CON of 15/239,398 08/17/2016 PAT 9641957
which is a CON of 14/979,233 12/22/2015 PAT 9532161
which is a CON of 14/667,353 03/24/2015 PAT 9232403
which is a CON of 14/263,604 04/28/2014 PAT 9037127
which is a CON of 12/380,780 03/02/2009 PAT 8839388
which claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 01/25/2022

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/577,237**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Automated Device Provisioning and Activation

Preliminary Class

370

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign

page 2 of 4

patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD						Application or Docket Number 17/577,237	
Substitute for Form PTO-875							
APPLICATION AS FILED - PART I							
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1	minus 20 = *	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1	minus 3 = *	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			840			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	
				1670			
APPLICATION AS AMENDED - PART II							
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		OTHER THAN SMALL ENTITY	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=
	Application Size Fee (37 CFR 1.16(s))						
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.							



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/577,237	01/17/2022	Gregory G. Raleigh	RALEP007C11C3C2C3C2C1C1C1

CONFIRMATION NO. 5850

FORMALITIES LETTER

106963
Headwater Research LLC
110 North College Avenue
Suite 1116
Tyler, TX 75702



Date Mailed: 01/27/2022

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
- The application search fee must be submitted.
- The application examination fee must be submitted.
- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.

The surcharge is due for any one of:

- late submission of the basic filing fee, search fee, or examination fee,
- late submission of inventor's oath or declaration,
- filing an application that does not contain at least one claim on filing, or
- submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- \$ **80** basic filing fee.
- \$ **840** for **160** electronically equivalent pages in excess of **100** application size fee.
- \$ **80** surcharge.
- \$ **350** search fee.
- \$ **400** examination fee.
- \$(**0**) previous unapplied payment amount.
- \$ **1750** TOTAL FEE BALANCE DUE.

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice".
<https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/elbanaybanay/

AUTOMATED DEVICE PROVISIONING AND ACTIVATION

BACKGROUND OF THE INVENTION

[0001] With the advent of mass market digital communications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), and Wi-Fi (Wireless Fidelity) wireless networks increasingly becoming user capacity constrained. Although wireless network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0002] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0004] FIG. 1 illustrates a simplified (e.g., “flattened”) network architecture in accordance with some embodiments.

[0005] FIG. 2 illustrates another simplified (e.g., “flattened”) network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments.

[0006] FIG. 3 illustrates another simplified (e.g., “flattened”) network architecture including two central providers in accordance with some embodiments.

[0007] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments.

[0008] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments.

[0009] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments.

[0010] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments.

[0011] FIG. 8 illustrates another simplified (e.g., “flattened”) network architecture including multiple wireless access networks (e.g., 3G and 4G Wireless Wide Area Networks (WWANs)) and multiple wire line networks (e.g., Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks) in accordance with some embodiments.

[0012] FIG. 9 illustrates a hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0013] FIG. 10 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0014] FIG. 11 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0015] FIG. 12 illustrates another hardware diagram of a device that includes a service processor in accordance with some embodiments.

[0016] FIG. 13 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0017] FIG. 14 illustrates another hardware diagram of a device that includes a service processor implemented in external memory of a System On Chip (SOC) in accordance with some embodiments.

[0018] FIGS. 15A through 15F illustrate hardware diagrams of a device that include a service processor and a bus structure extension using intermediate modem or networking device combinations in accordance with various embodiments.

[0019] FIG. 16 is a functional diagram illustrating a device based service processor and a service controller in accordance with some embodiments.

[0020] FIG. 17 is another functional diagram illustrating the device based service processor and the service controller in accordance with some embodiments.

[0021] FIG. 18 is another functional diagram illustrating the device based service processor and the service controller in which the service processor controls the policy implementation for multiple access network modems and technologies in accordance with some embodiments.

[0022] FIG. 19 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0023] FIG. 20 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0024] FIG. 21 is another functional diagram illustrating the service processor and the service controller in accordance with some embodiments.

[0025] FIGS. 22A and 22B provide tables summarizing various service processor agents (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0026] FIG. 23 provides a table summarizing various service controller server elements (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments.

[0027] FIG. 24 is a functional diagram illustrating the service control device link of the service processor and the service control service link of the service controller in accordance with some embodiments.

[0028] FIG. 25 is a functional diagram illustrating framing structure of a service processor communication frame and a service controller communication frame in accordance with some embodiments.

[0029] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters in accordance with some embodiments.

[0030] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments.

[0031] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments.

[0032] FIG. 29 is a functional diagram illustrating a device communications stack that allows for implementing verifiable traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0033] FIG. 30 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0034] FIG. 31 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0035] FIG. 32 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0036] FIG. 33 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0037] FIG. 34 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0038] FIG. 35 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0039] FIG. 36 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0040] FIG. 37 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments.

[0041] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments.

[0042] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0043] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments.

[0044] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments.

[0045] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments.

[0046] FIGS. 43A through 43B are flow diagrams illustrating a flow diagram for a service processor authorization sequence as shown in FIG. 43A and a flow diagram for a service controller authorization sequence as shown in FIG. 43B in accordance with some embodiments.

[0047] FIGS. 44A through 44B are flow diagrams illustrating a flow diagram for a service processor activation sequence as shown in FIG. 44A and a flow diagram for a service controller activation sequence as shown in FIG. 44B in accordance with some embodiments.

[0048] FIGS. 45A through 45B are flow diagrams illustrating a flow diagram for a service processor access control sequence as shown in FIG. 45A and a flow diagram for a service controller access control sequence as shown in FIG. 45B in accordance with some embodiments.

[0049] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0050] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments.

[0051] FIG. 48 illustrates a network architecture including a service controller device control system and a service controller analysis and management system in accordance with some embodiments.

[0052] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments.

[0053] FIG. 50 illustrates a network architecture including a billing to service controller interface for accommodating minimum changes in existing central billing, AAA and/or other network components in accordance with some embodiments.

[0054] FIG. 51 illustrates a network architecture for locating service controller device control functions with AAA and network service usage functions in accordance with some embodiments.

[0055] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments.

[0056] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments.

[0057] FIG. 54 illustrates a network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0058] FIG. 55 illustrates another network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments.

[0059] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0060] FIG. 57 illustrates a network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0061] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments.

[0062] FIG. 59 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0063] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0064] FIG. 61 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0065] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments.

[0066] FIG. 63 illustrates another network architecture including the VSP workstation server in communication with the 4G/3G/2G DPI/DPC gateways in accordance with some embodiments.

[0067] FIG. 64 illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments.

DETAILED DESCRIPTION

[0068] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term “processor” refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0069] A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0070] With the development and increasing proliferation of mass market digital communications and content distribution, communication network capacity gains are being outpaced by growing digital networking demand. For example, some industry experts project average wireless device usage of four devices per subscriber, with a mixture of general purpose devices like smart phones and computers along with special purpose devices like music players, electronic readers, connected (e.g., networked) cameras and connected gaming devices. In

addition, wire line user service consumption habits are trending toward very high bandwidth applications that can quickly consume the available capacity and degrade overall network service experience if not efficiently managed. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

[0071] There is a need for a communication system and method that provides for flexible service plans and management of user network services to provide consumer choice of more refined service plan offerings and efficient management of network capacity.

[0072] Also, it is becoming increasingly important to more deeply manage the level of services delivered to networked devices to provide cost effective services that match growing digital networking usage patterns. For example, access providers can move away from only billing for basic access and move toward billing for higher level service delivery with example services including rich Internet access and email, application based billing, content distribution, entertainment activities, information or content subscription or gaming. In addition, a growing number of new special purpose and general purpose networked devices are fueling demand for new service plans, for example, tailored to the new device usage models (e.g., a special service plan for an e-book reader device).

[0073] As network capabilities grow and new networked device offerings grow, access network service providers will realize increasing value in opening up their networks to allow innovation and expanded offerings for network service consumers. However, opening up the networks to provide efficient third party definition of alternative service and billing models requires more flexible service and billing policy management solutions. For example, machine to machine applications such as telemetry, surveillance, shipment tracking and two way power control systems are example new applications that would require new offerings to make such available to network service customers. The need to customize service offerings for these new applications requires more efficient methods for defining, testing and launching new services with more refined control of service functions and service costs. In some embodiments, this means billing for different types of service elements, such as total traffic, content downloads, application usage, information or content subscription services, people or asset tracking services, real time machine to machine information or electronic commerce transactions.

[0074] In some embodiments, network user capacity is increased and user service costs are reduced by managing and billing for service consumption in a more refined manner (e.g., to satisfy network neutrality requirements). By managing service consumption in a user friendly manner, the overall service capacity required to satisfy the user device needs can be tailored more closely to the needs of a given user thereby reducing user service costs and increasing service provider profits. For example, managing service usage while maintaining user satisfaction includes service usage policy implementation and policy management to identify, manage and bill for service usage categories, such as total traffic consumption, content downloads, application usage, information or content subscription services, electronic commerce transactions, people or asset tracking services or machine to machine networking services. As described herein, service activity is used to refer to any service usage or traffic usage that can be associated with, for example, an application; a network communication end point, such as an address, uniform resource locator (URL) or other identifier with which the device is communicating; a traffic content type; a transaction where content or other material, information or goods are transacted, purchased, reserved, ordered or exchanged; a download, upload or file transfer; email, text, SMS, IMS or other messaging activity or usage; VOIP services; video services; a device usage event that generates a billing event; service usage associated with a bill by account activity (also referred to as billing by account) as described herein; device location; device service usage patterns, device user interface (UI) discovery patterns, content usage patterns or other characterizations of device usage; or other categories of user or device activity that can be identified, monitored, recorded, reported, controlled or processed in accordance with a set of verifiable service control policies. As will be apparent to one of ordinary skill in the art in view of the embodiments described herein, some embodiments identify various service activities for the purpose of decomposing overall service usage into finer sub-categories of activities that can be verifiably monitored, categorized, cataloged, reported, controlled, monetized and used for end user notification in a manner that results in superior optimization of the service capabilities for various levels of service cost or for various types of devices or groups. In some embodiments, it will be apparent to one of ordinary skill in the art that the terms service activity or service usage are associated with categorizing and possibly monitoring or controlling data traffic, application usage, communication with certain network end points, or transactions, and it will also be apparent that in some embodiments the term service activity is

intended to include one or more of the broader aspects listed above. The shortened term service usage can be used interchangeably with service activity, but neither term is intended in general to exclude any aspect of the other. In some cases, where the terms service usage or service activity are used, more specific descriptors such as traffic usage, application usage, website usage, and other service usage examples are also used to provide more specific examples or focus in on a particular element of the more encompassing terms.

[0075] In some embodiments, employing this level of service categorization and control is accomplished in a manner that satisfies user preferences. In some embodiments, employing this level of service categorization and control is accomplished in a manner that also satisfies government rules or regulations regarding open access, for example, network neutrality requirements. In some embodiments, service management solutions that also collect and/or report user or device service usage or service activity behavior to determine how best to meet the user's simultaneous desires for service quality and lower service costs are disclosed. For example, such monitoring and reporting are accomplished in a manner that includes approval by the user and in a manner that also protects the privacy of user information and service usage behavior or service activity history.

[0076] In some embodiments, a system and method is disclosed for increasing network user capacity for wireless networks in the face of increasing service demand per user by providing for a greater number of base stations, also sometimes referred to as access points, base terminals, terminal nodes or other well known acronyms, to be more easily and/or more cost effectively deployed. For example, to simplify the process of deploying base stations, the installation complexity and the network infrastructure required for the base station to obtain backhaul service to the various networks that users desire to connect with are reduced.

[0077] In some embodiments, dense base station deployments are simplified by reducing the requirement to aggregate or concentrate the base station traffic through a specific dedicated core network infrastructure, so that the base stations connect to the desired user networks through a more diverse set of local loop, back bone and core routing options. This approach also reduces network infrastructure equipment, installation and maintenance costs. In some embodiments, this is accomplished by distributing the network traffic policy implementation and

control away from the core network by providing for more control for service policy implementation and management on the end user device and, in some embodiments, in the end user device with respect to certain service policies and the network (e.g., control plane servers) with respect to other service policies. For example, this approach facilitates connecting the base stations directly to the local loop Internet with a minimum of specific dedicated networking infrastructure.

[0078] In some embodiments, service and transaction billing event capture and logging are distributed to the device. For example, providing service and transaction billing event capture and logging at the device provides a greater capability to monitor, classify and control deeper aspects of service usage or service activity at the device as compared to the relatively less capability for the same in the network infrastructure (e.g., for certain traffic flows, such as encrypted traffic flows). Furthermore, billing at the device provides for very specialized with many different billing and service plans for different device and service usage or service activity scenario combinations without the problem of attempting to propagate and manage many different deep packet inspection (DPI) and traffic shaping profiles in the networking equipment infrastructure. For example, service billing at the device can provide for more sophisticated, more specialized and more scalable billing and service plans.

[0079] Another form of billing that needs improvement is electronic commerce transaction billing with device assisted central billing. Today, most central billing and content distribution models require either centralized content distribution maintained by the central service provider or central billing authority, or a centralized ecommerce website or portal traffic aggregation system controlled by the central service provider or central billing provider, or both. In such systems, content and transaction providers such as media providers, application developers, entertainment providers, transaction website providers and others must adapt their mainstream electronic offering and commerce systems, such as shopping experience websites, to fit within the various proprietary customized infrastructure and content storage solutions for ecommerce markets, such as BREW® (Binary Runtime Environment for Wireless from Qualcomm® Inc.), Symbian OS (from Symbian Software Ltd) and Apple iPhone 3G App Store (from Apple Inc.). This approach requires a large amount of unnecessary custom interface development and stifles open market creativity for HTTP, WAP or portal/widget based shopping

destinations and experiences. As disclosed below, a superior approach includes device based transaction billing for an open ecosystem in which a central billing provider provides users and ecommerce transaction providers with a central billing solution and experience that does not require extensive custom development or ecommerce infrastructure interfacing.

[0080] In some embodiments, products that incorporate device assisted service policy implementation, network services and service profiles (e.g., a service profile includes a set of one or more service policy settings for the device for a service on the network) are disclosed, as described below. For example, aspects of the service policy (e.g., a set of policies/policy settings for the device for network services, typically referring to lower level settings, such as access control settings, traffic control settings, billing system settings, user notification settings, user privacy settings, user preference settings, authentication settings and admission control settings) that are moved out of the core network and into the end user device include, for example, certain lower level service policy implementations, service usage or service activity monitoring and reporting including, for example, privacy filtering, customer resource management monitoring and reporting including, for example, privacy filtering, adaptive service policy control, service network access control services, service network authentication services, service network admission control services, service billing, transaction billing, simplified service activation and sign up, user service usage or service activity notification and service preference feedback and other service capabilities.

[0081] As discussed below, product designs that move certain aspects of one or more of these service profile or service policy implementation elements into the device provide several advantageous solutions to the needs described above. For example, benefits of certain embodiments include the ability to manage or bill for a richer and more varied set of network services, better manage overall network capacity, better manage end user access costs, simplify user or new device service activation, simplify development and deployment of new devices with new service plans (e.g., service profile and billing/costs information associated with that service profile), equip central service providers with more effective open access networks for new third party solutions, simplify the equipment and processes necessary to deploy wireless base stations and simplify the core networking equipment required to deploy certain access networks.

[0082] As discussed below, there are two network types that are discussed: a central provider network and a service provider network. The central provider network generally refers to the access network required to connect the device to other networks. The central provider network generally includes the physical layer, the Media Access Control (MAC) and the various networking functions that can be implemented to perform authentication, authorization and access control, and to route traffic to a network that connects to the control plane servers, as discussed below. The service provider network generally refers to the network that includes the control plane servers. In some embodiments, a central provider network and a service provider network are the same, and in some embodiments, they are different. In some embodiments, the owner or manager of the central provider network and the owner or manager of the service provider network are the same, and in some embodiments, they are different.

[0083] In some embodiments, control of the device service policies is accomplished with a set of service control plane servers that reside in the access network or any network that can be reached by the device. This server based control plane architecture provides for a highly efficient means of enabling third party control of services and billing, such as for central carrier open development programs or Mobile Virtual Network Operator (MVNO) relationships. As device processing and memory capacity expands, moving to this distributed service policy processing architecture also becomes more efficient and economical. In some embodiments, several aspects of user privacy and desired network neutrality are provided by enabling user control of certain aspects of device based service usage or service activity reporting, traffic reporting, service policy control and customer resource management (CRM) reporting.

[0084] In many access networks, such as wireless access networks, bandwidth capacity is a valuable resource in the face of the increasing popularity of devices, applications and content types that consume more bandwidth. To maintain reasonable service profit margins, a typical present service provider practice is to charge enough per user for access to make service plans profitable for the higher bandwidth users. However, this is not an optimal situation for users who desire to pay less for lower bandwidth service usage or service activity scenarios.

[0085] Accordingly, in some embodiments, a range of service plan pricing can be enabled that also maintains service profitability for the service provider, for example, by

providing a more refined set of management and control capabilities for service profiles. For example, this approach generally leads to service management or traffic shaping where certain aspects of a service are controlled down based on service policies to lower levels of quality of service. Generally, there are three problems that arise when these techniques are implemented. The first problem is maintaining user privacy preferences in the reporting of service usage or service activity required to set, manage or verify service policy implementation. This problem is solved in a variety of ways by the embodiments described below with a combination of user notification, preference feedback and approval for the level of traffic information the user is comfortable or approves and the ability to filter service usage or service activity, in some embodiments, specifically traffic usage or CRM reports so that only the level of information the user prefers to share is communicated. The second problem is satisfying network neutrality requirements in the way that traffic is shaped or services are managed. This problem is solved in a variety of ways as described in the embodiments described below by empowering the user to make the choices on how service usage, service activity, traffic usage or CRM data is managed down to control costs, including embodiments on user notification and service policy preference feedback. By allowing the user to decide how they want to spend and manage their service allowance or resources, a more neutral or completely neutral approach to network usage can be maintained by the service provider. The third problem is to help the user have an acceptable and enjoyable service experience for the lower cost plans that will result in much wider scale adoption of connected devices and applications but are more constrained on service activity usage or options or bandwidth or traffic usage. As lower cost service plans are offered, including plans where the basic connection service may be free, these service plans will require service provider cost controls to maintain profitability or preserve network capacity that result in lower limits on service usage or service activity. These lower service usage or service activity limit plans will result in more users who are likely run over service usage limits and either experience service shutdown or service cost overages unless they are provided with more capable means for assistance on how to use and control usage for the lower cost services. This problem is solved in a variety of ways with a rich collection of embodiments on user notification, service usage and cost projection, user notification policy feedback, user service policy preference feedback, and adaptive traffic shaping or service policy implementation. As described herein, some embodiments allow a wide range of flexible and verifiable service plan and service profile

implementations ranging from examples such as free ambient services that are perhaps sponsored by transaction revenues and/or bill by account sponsored service partner revenues, to intermediately priced plans for basic access services for mass market user devices or machine to machine communication devices, to more expensive plans with very high levels of service usage or service activity limits or no limits at all. Several bill by account embodiments also provide for the cataloging of service usage that is not a direct benefit to end users but is needed for basic maintenance of the device control channels and access network connection, so that the maintenance traffic service cost can be removed from the user billing or billed to non-user accounts used to track or account for such service costs. These embodiments and others result in a service usage or service activity control capability that provides more attractive device and service alternatives to end users while maintaining profitability for service providers and their partners.

[0086] In some embodiments, the above described various embodiments for device based service policy and/or service profile communications control are implemented using network based service control, for example, for satisfying various network neutrality and/or privacy requirements, based on indication(s) received from the device (e.g., user input provided using the device UI using the service processor) and network based service control (e.g., using a DPI service monitor or DPC policy implementation and/or other network elements).

[0087] In some embodiments, a virtual network overlay includes a device service processor, a network service controller and a control plane communication link to manage various aspects of device based network service policy implementation. In some embodiments, the virtual network overlay networking solution is applied to an existing hierarchical network (e.g., for wireless services), and in some embodiments, is applied to simplify or flatten the network architecture as will be further described below. In some embodiments, the large majority of the complex data path network processing required to implement the richer service management objectives of existing hierarchical networks (e.g., for wireless services) are moved into the device, leaving less data path processing required in the edge network and in some cases even less in the core network. Because the control plane traffic between the service control servers and the device agents that implement service policies can be several orders of magnitude slower than the data plane traffic, service control server network placement and back-haul

infrastructure is much less performance sensitive than the data plane network. In some embodiments, as described further below, this architecture can be overlaid onto all the important existing access network architectures used today. In some embodiments, this architecture can be employed to greatly simplify core access network routing and data plane traffic forwarding and management. For example, in the case of wireless networks, the incorporation of device assisted service policy implementation architectures can result in base stations that directly connect to the Internet local loop and the data traffic does not need to be concentrated into a dedicated core network. This results, for example, in a large reduction in backhaul cost, core network cost and maintenance cost. These cost savings can be re-deployed to purchase and install more base stations with smaller cells, which results in higher data capacity for the access network leading to better user experience, more useful applications and lower service costs. This flattened networking architecture also results in latency reduction as fewer routes are needed to move traffic through the Internet. In some embodiments, the present invention provides the necessary teaching to enable this powerful transformation of centralized network service architectures to a more distributed device based service architectures.

[0088] Device based billing can be compromised, hacked and/or spoofed in many different ways. Merely determining that billing reports are being received from the device, that the device agent software is present and properly configured (e.g., the billing agent is present and properly configured) is insufficient and easily spoofed (e.g., by spoofing the agent itself, providing spoofed billing reports using a spoofed billing agent or providing spoofed agent configurations). Accordingly, in some embodiments, verifiable device assisted and/or network based service policy implementation is provided. For example, verifiable service usage and/or service usage billing can be provided as described herein with respect to various embodiments.

[0089] While much of the below discussion and embodiments described below focus on paid service networks, those of ordinary skill in the art will appreciate that many of the embodiments also apply to other networks, such as enterprise networks. For example, the same device assisted network services that create access control services, ambient activation services and other service profiles can be used by corporate IT managers to create a controlled cost service policy network for corporate mobile devices. As another example, embodiments described below for providing end user service control can also allow a service provider to offer

parental controls by providing parents with access to a website with a web page that controls the policy settings for the access control networking service for a child's device.

Network Architecture for Device Assisted/Based Service Control

[0090] FIG. 1 illustrates a simplified (e.g., “flattened”) network architecture in accordance with some embodiments. As shown, this provides for a simplified service infrastructure that exemplifies a simplified and “flattened” network architecture in accordance with some embodiments that is advantageous for wireless network architectures. This also reduces the need for complex data path protocol interaction between the base station and network infrastructure. For example, in contrast to a complex edge and core network infrastructure connecting base stations to the central service provider network, as shown the base stations 125 are connected directly to the Internet 120 via firewalls 124 (in some embodiments, the base stations 125 include the firewall functionality 124). Accordingly, in some embodiments, a central provider network is no longer required to route, forward, inspect or manipulate data plane traffic, because data plane traffic policy implementation is conducted in the device 100 by the service processor 115. However, it is still an option, in some embodiments, to bring data plane traffic in from the base stations 125 to a central provider network using either open or secure Internet routing if desired. Base station control plane communication for access network AAA (Authentication, Authorization, and Accounting) server 121, DNS/DHCP (Domain Name System/Dynamic Host Configuration Protocol) server 126, mobile wireless center 132 (sometimes referenced to in part as a home location register (HLR) or other acronym) or other necessary functions are accomplished, for example, with a secure IP tunnel or TCP connection between the central provider network and the base stations. The base station 125 is used to refer to multiple base station embodiments where the base station itself is directly connected to the RAN, or where the base station connects to a base station controller or base station aggregator function that in turn connects to the RAN, and all such configurations are collectively referred to herein as base station 125 in FIG. 1 and most figures that follow that reference base station 125 as described below.

[0091] As shown, the central provider access network is both 3G and 4G capable, the devices 100 can be either 3G, 4G or multi-mode 3G and 4G. Those of ordinary skill in the art

will also appreciate that in the more general case, the network could be 2G, 3G and 4G capable, or the device could be 2G, 3G and 4G capable with all or a subset of Global System for Mobile (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA) 1X, High Speed Packet Access (HSPA), Evolution Data Optimized (EVDO), Long Term Evolution (LTE) and WiMax modem capability. If the devices are single mode, then the 3G devices 100 will be activated with a service profile applied to service processor 115 that is consistent with the 3G network capacity and speed, and the 4G devices will be activated with service profiles applied to service processor 115 that are consistent with 4G network capacity and speed. In both cases, the same service controller 122 manages services for both sets of devices in accordance with some embodiments. If the devices are multimode, then the service processor 115 can be activated with a dual mode service profile capability in which the service profile for 3G offers a similar rich set of services as the service profile for 4G but with, for example, scaled back bandwidth. For example, this approach is allows central providers to offer a richer set of service offerings with 3G and then migrate the same set of service offerings to 4G but with higher performance. In particular, this approach allows 3G to 4G rich service migration to occur, for example, with the only change being the increased bandwidth settings in the service profiles that will be available in 4G at the same cost as 3G with lower service profile bandwidth settings.

[0092] In some embodiments, if the devices are multimode, a network selection policy implementation within service processor 115 is provided, or in some embodiments, a network selection policy is driven by policy decisions made in service controller 122 based on service availability reports received from service processor 115. The network selection policy allows the selection of the network that corresponds to the most desirable service profile to meet the user's service preferences. For example, if the user specifies, within the framework of the service notification and user preference feedback embodiments described below, that maximum performance is the most important factor in selecting which access network to connect to, then the best profile is likely to be the 4G network as 4G is typically faster, except perhaps, for example, if the device 100 is closer to the 3G base station so that there is a much stronger signal or if the 4G network is much more heavily loaded than the 3G network. On the other hand, if the user preference set specifies cost as the most important factor, then depending on the central provider service costs the 3G network may prove to be the most desirable service profile. This is

a simple example and many other selection criteria are possible in the network selection embodiment as discussed further below.

Network Based Service Usage Monitoring for Verification and Other Purposes

[0093] In some embodiments, if the base station data plane traffic is transmitted via the Internet 120 as discussed above, then IPDRs (Internet Protocol Detail Records, also sometimes and interchangeably referred to herein as Charging Data Records or CDRs, which as used herein refer to any network measure of service usage or service activity for voice and/or data traffic (e.g., IPDRs can include a time stamp, a device ID, and various levels of network measures of service usage for the device associated with that device ID, such as perhaps total traffic usage, network destination, time of day or device location)) are generated by and collected from the access network equipment. Depending on the specific network configuration, as discussed herein, for a WWAN network the IPDRs can be generated by one or more of the following: base station 125, RAN or transport gateways and AAA 121. In some access network embodiments, the IPDRs are transmitted to equipment functions that aggregated the IPDRs for the purpose of service billing and other functions. Aggregation can occur in the AAA, the transport gateways or other functions including the billing system 123. As discussed below, it is often the case that the IPDRs is assumed to be obtained from the AAA server 121 and/or a service usage data store 118 (e.g., a real-time service usage collection stored in a database or a delayed feed service usage collection stored in a database), or some other network function. However, this does not imply that the IPDRs may not be obtained from a variety of other network functions, and in some embodiments, the IPDRs are obtained from other network functions as disclosed herein. In some embodiments, existing IPDR sources are utilized to obtain network based service usage measures for multiple purposes including but not limited to service policy or profile implementation verification, triggering service verification error responds actions, and service notification synchronization. Certain types of IPDRs can be based on, or based in part on, what are sometimes referred to as CDRs (Charging Data Records, which can track charges for voice and data usage) or modifications of CDRs. Although the capability to monitor, categorize, catalog, report and control service usage or service activity is in general higher on the device than it is in the network, and, as described herein, device based service monitoring or control assistance is in some ways desirable as compared to network based implementations, as described herein many

embodiments take advantage of network based service monitoring or control to augment device assisted service monitoring or control and vice versa. For example, even though many embodiments work very well with minimal IPDR service usage or service activity information that is already available in a network, deeper levels of IPDR packet inspection information in general enable deeper levels of service monitoring or service control verification, which can be desirable in some embodiments. As another example, deeper levels of network capability to control service usage or service activity can provide for more sophisticated error handling in some embodiments, for example, providing for more options of the Switched Port Analyzer (SPAN) and network quarantine embodiments as described herein. As another example, in some embodiments it is advantageous to take advantage of network based service monitoring or control for those service aspects the network is capable of supporting, while using device assisted service monitoring or control for the service aspects advantageously implemented on the device.

[0094] In some embodiments, where base station data plane traffic is backhauled and concentrated in a central provider core network 110, then the IPDRs can originate in the base stations or a router or gateway in the central provider network 110, and the IPDRs are collected at the AAA server 121 and stored in the service usage data store 118. In some embodiments, the central billing system 123 collects the IPDRs from the AAA server 121 for service billing accounting purposes. In some embodiments, a central billing system 123 collects the IPDRs directly from the initial IPDR source or some other aggregator. In some embodiments, outside partners like MVNOs gain access to the IPDRs from the central billing system 123. As discussed below, it is assumed that the IPDRs are obtained from the AAA server 121, and it is understood that the source of the IPDRs is interchangeable in the embodiments.

[0095] In some embodiments, the IPDR information is used by the service processor 115, the service controller 122 and/or other network apparatus or device apparatus to implement service control verification is provided as described below. In some embodiments, an IPDR feed (e.g., also referred to as a charging data record (CDR)) flows between network elements. For example, an IPDR feed can flow from the RAN gateway 410 (e.g., SGSN 410, BSC packet control 510 or RNC 512) and the transport gateway 420 (e.g., GGSN or PDSN). In other embodiments, the IPDRs originate and flow from the base station 125 or some other

component/element in the network. In some embodiments, one or more of these IPDR feeds is transmitted to an IPDR aggregation function (e.g., also referred to as a charging gateway). For example, this aggregation function can be located in the AAA 121, in the mobile wireless center 132 (and/or in the home location register (HLR) or other similar function referred to by other common industry names), in the transport gateway 420, or in some other network element. This aggregation function collects the IPDR feeds into a database with an entry for each device 100. In some embodiments, an intermediate aggregation function is provided that feeds a higher level aggregation function, for example, the transport gateway 420 can receive IPDR feeds from the RAN gateway 410 or the base station 125 before sending them to another aggregation function. At some point in time (e.g., at the end of a specified time period, at the end of a device network connection session and/or at a specified time of day), the IPDR aggregation function sends summary information or detailed information of the IPDRs for a given device or group of devices to the billing system for billing and/or reconciliation. In some embodiments, in which the IPDR aggregation feed to the billing system is frequent enough for one or more of the IPDR information purposes described herein, the IPDR feed for the service controller 122 is derived from the aggregated feed, either by having the billing system 123 transmit it to the service controller 122, or by copying it from the IPDR aggregation function.

[0096] In some embodiments, the IPDR feed is obtained from the network function that is generating or aggregating the IPDR feed as described herein. In some embodiments, the IPDR feed is copied from the aggregation function in a manner that does not interrupt the operation of the network. For example, a switch based port analysis function can be used to copy the traffic to a traffic analysis or server element that filters out the IPDR traffic and records it to a data base that is then either pushed to the service controller 122 (or any other network element that uses IPDR information as described herein), or is queried by the service controller 122 (or any other function that uses the IPDR information as described herein). In some embodiments, if the aggregated IPDR information transmitted to the billing system is delayed from real-time traffic usage events by an amount of time that is, for example, too long for desired operation, or for any other reason that makes it less desirable to obtain the IPDR information from the same aggregated feed used for the billing system 123, the IPDR information can be collected from one or more of the sources discussed above including, for example, from another aggregation point (e.g., the feed to the charging gateway, AAA server and/or mobile wireless center/HLR), one or

more of the gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720 the base station 125 and/or another network element. In some embodiments, the IPDR feeds from these or other network functions are copied to a database as described above, which is either pushed or queried to get the information to the service controller 122 or other network elements that request the IPDR information.

[0100] In some embodiments, the service processor 115 includes various components, such as device agents, that perform service policy implementation or management functions. In some embodiments, these functions include service policy or implementation verification, service policy implementation tamper prevention, service allowance or denial, application access control, traffic control, network access control services, various network authentication services, service control plane communication, device heartbeat services, service billing, transaction billing, simplified activation services and/or other service implementations or service policy implementations. It will be apparent to those of ordinary skill in the art that the division in functionality between one device agent and another is a design choice, that the functional lines can be re-drawn in any technically feasible way that the product designers see fit, and that the placing divisions on the naming and functional breakouts for device agents aids in understanding, although in more complex embodiments, for example, it can make sense to the product designer to break out device agent functionality specifications in some other manner in order to manage development specification and testing complexity and workflow.

[0101] In some embodiments, network control of the service policy settings and services as discussed above is accomplished with the service controller 122 which in various embodiments includes one or more server functions. As with the service processor 115 agent naming and functional break out, it is understood that service controller 122 server naming and functional breakout is also a design choice and is provided mainly to aid in the discussion. It will be apparent to those of ordinary skill in the art that the server names and functional breakouts do not imply that each name is an individual server, and, for example, a single named function in the various embodiments can be implemented on multiple servers, or multiple named functions in the various embodiments can be implemented on a single server.

[0102] As shown, there are multiple open content transaction partner sites 134 (e.g., open content transaction servers), which represent the websites or experience portals offered by content partners or ecommerce transaction partners of the service provider. For example, transaction servers 134 can provide an electronic commerce offering and transaction platform to the device. In some embodiments, the central provider has ownership and management of the service controller 122, so the central provider and the service provider are the same, but as discussed below the service provider that uses the service controller 122 to manage the device services by way of service processor 115 is not always the same as the central provider who provides the access network services.

[0103] In some embodiments, further distribution of central provider access networking functions such as access network AAA server 121, DNS/DHCP server 126, and other functions are provided in the base stations 125. In some embodiments, network based device service suspend/resume control are also provided in the base stations 125 (or in some embodiments, for hierarchical or overlay networks, this function is provided by one or more of the following: RAN gateways, transport gateways, AAA 121 or some other network function). As shown, the following are connected (e.g., in network communication with) the central provider network 110: central provider billing system 123, dedicated leased lines 128 (e.g., for other services/providers), central provider service controller 122, a content management (e.g., content switching, content billing, and content catching) system 130, central provider DNS/DHCP server 126, access network AAA server 121, service usage data store 118 and central provider mobile wireless center 132. These embodiments may be advantageous particularly for flat networks as that shown in FIG. 1 that are provided by the present invention.

[0104] In some embodiments, the base stations 125 implement a firewall function via firewall 124 and are placed directly onto the local loop Internet for backhaul. Voice traffic transport is provided with a secure protocol with Voice Over IP (VOIP) framing running over a secure IP session, for example, Virtual Private Network (VPN), IP Security (IPSEC) or another secure tunneling protocol. In some embodiments, the VOIP channel employs another layer of application level security on the aggregated VOIP traffic trunk before it is placed on the secure IP transport layer. Base station control traffic and other central provider traffic can be provided in a number of ways with secure transport protocols running over Transmission Control Protocol

(TCP), Internet Protocol (IP) or User Datagram Protocol (UDP), although TCP provides a more reliable delivery channel for control traffic that is not as sensitive to delay or jitter. One example embodiment for the control channel is a control link buffering, framing, encryption and secure transport protocol similar to that described below for the service control link between a device and the network. In some embodiments, a service control heartbeat function is provided to the base stations 125 similar to that implemented between the service controller 122 and the service processor 115 as described below. If the need to maintain a bandwidth efficient control plane channel between the base stations and the central provider base station control network is not as critical as it is in the case of access network connection to the device, then there are many other approaches for implementing a secure control channel over the Internet including, for example, one or more of various packet encryption protocols running at or just below the application layer, running TCP Transport Layer Security (TLS), and running IP level security or secure tunnels.

[0105] In some embodiments, the device based services control plane traffic channel between the service processor 115 and the service controller 122 is implemented over the same control plane channel used for the flat base station control architecture, or in some embodiments, over the Internet. As discussed below, it is assumed that the device bases services control plane channel for service processor 115 to service controller 122 communications is established through the Internet 120 or through the access network using IP protocols as this is the more general case and applies to overlay network applications for various embodiments as well as applications where various embodiments are used to enable flattened access networks.

[0106] In some embodiments, by enabling the device to verifiably implement a rich set of service features as described herein, and by enabling the base station 125 to connect directly to the Internet 120 with a local firewall for device data traffic, tunnel the voice to a voice network with VOIP and secure Internet protocols, and control the base station 125 over a secure control plane channel using base station control servers located in a central provider network, base stations 125 can be more efficiently provisioned and installed, because, for example, the base station 125 can accommodate a greater variety of local loop backhaul options. In such embodiments, it is advantageous to perform certain basic network functions in the base station 125 rather than the central provider network.

[0107] In some embodiments, a basic device suspend/resume function for allowing or disallowing the device Internet access is provided by the base stations 125 (or in some embodiments, for hierarchical or overlay networks in some embodiments this function is provided by one or more of the following: RAN gateways, transport gateways, AAA 121 or some other network function). This functionality, as will be discussed below, is important for certain embodiments involving taking action to resolve, for example, service policy verification errors. In some embodiments, this function is performed at the base station (e.g., base stations 125) thereby eliminating the need for a more complex networking equipment hierarchy and traffic concentration required to perform the suspend/resume function deeper in the network. Access network base stations control media access and are therefore designed with awareness of which device identification number a given traffic packet, group of packets, packet flow, voice connection or other traffic flow originates from and terminates to. In some embodiments, the suspend/resume function is implemented in the base station 125 by placing an access control function in the traffic path of each device traffic flow. The suspend resume function can be used by various network elements, and in the context of the present embodiment can be used by the service controller 122 (e.g., in some embodiments, access control integrity server 1654 (FIG. 16) of service controller 122 or other service controller elements) to suspend and resume device service based on the assessment of the service policy implementation verification status as described below.

[0108] In some embodiments, at least a basic traffic monitoring or service monitoring function is performed at the base station (e.g., base stations 125) similar to the service history records or IPDRs collected deeper in the network in more conventional hierarchical access network infrastructure architectures. For example, the service or traffic monitoring history records are advantageous for tracking device network service usage or service activity behavior and for certain verification methods for device based service policy implementation or higher device based services as discussed below. In some embodiments, a traffic monitoring function is provided in the base station 125 in which the traffic for each device is at least counted for total traffic usage and recorded. In some embodiments, traffic inspection beyond simply counting total traffic usage is provided. For example, the base station traffic monitor can record and report IP addresses or include a DNS lookup function to report IP addresses or IP addresses and associated Uniform Resource Locators (URLs). Another example allows the base station 125 to

attach location data to the IPDR to provide device location data in the records. In some embodiments, traffic inspection includes recording deeper levels of traffic or service monitoring.

[0109] In some embodiments, device traffic associated with service verification conditions indicating service usage is out of policy or profile limits or allowances is routed to a quarantine network rather than or as an initial alternative to a suspending service. For example, the advantages for this approach and a more detailed description of the quarantine network are discussed below. In some embodiments, the quarantine network capability is provided for in which rather than simply suspending device traffic completely from the network as described above, the base station 125 includes a firewall function (e.g., firewall 124) that is capable of passing device access traffic with the quarantine network destinations and blocking device access to all other destinations. In some embodiments, when it is discovered that service verification conditions indicate that service usage is out of policy or profile limits or allowances, then one or more of the following actions are taken: the user is notified of the overage condition, the user is required to acknowledge the overage condition, the user account is billed for the overage condition, and the device is flagged for further analysis by a network device analysis function or a network manager.

[0110] In some embodiments, network complexity is reduced using the device without moving completely to a flat base station network as described above. Device participation in the core network services implementation provides for numerous measures for simplifying or improving network architecture, functionality or performance. For example, two approaches are discussed below ranging from a simple overlay of the service processor 115 onto devices and the service controller 122 in a conventional hierarchical access network as illustrated in FIGS. 4 through 7, to a completely flat network as illustrated in FIGS. 1 through 3 and 8. Those of ordinary skill in the art will appreciate that the disclosed embodiments provided herein can be combined with the above embodiments and other embodiments involving flat network base stations to provide several advantages including, for example, richer service capability, less access network complexity, lower access network expenses, more flexible base station deployments, or less complex or less expensive base station back haul provisioning and service costs.

[0111] In most of the discussion that follows, the network based service history records and the network based suspend-resume functionality used in certain embodiments involving service implementation verification are assumed to be derived from the device service history 1618 (as shown in FIG. 16) central provider network element and the AAA server 121 central provider network element, and in some embodiments, working in conjunction with other central provider network elements. It is understood that these functions provided by the network can be rearranged to be provided by other networking equipment, including the base station as discussed above. It is also understood that the network based device traffic monitoring, recording and reporting to the device service history 1618 element can be accomplished at the base stations. Furthermore, it is understood that while the AAA server 121 is assumed to provide the suspend/resume functionality, quarantine network routing or limited network access called for in some embodiments, the AAA server 121 can be a management device in which the actual implementation of the traffic suspend/resume, firewall, routing, re-direction forwarding or traffic limiting mechanisms discussed in certain embodiments can be implemented in the base stations as discussed above or in another network element.

[0112] In some embodiments, an activation server 160 (or other activation sequencing apparatus) provides for provisioning, as described below, of the devices 100 and/or network elements in the central provider network so that, for example, the device credentials can be recognized for activation and/or service by the network. In some embodiments, the activation server 160 provides activation functions, as described below, so that, for example, the devices can be recognized by the network, gain access to the network, be provided with a service profile, be associated with a service account and/or be associated with a service plan. As shown in FIG. 1, the activation server 160 is connected to the central provider core network 110. In this configuration, the activation server 160 acts as, an over the network or over the air, activation function. In some embodiments, the activation server 160, or variations of the activation server 160 as described below, is connected to apparatus in the manufacturing or distribution channel, or over the Internet 120, or as part of the service controller 122 to service provisioning or activation functions. In some embodiments, the activation server 160 is connected to the central provider core network 110. In some embodiments, the activation server 160 is connected to other network extensions such as an MVNO network or the Internet 120 if, for example, the routers in the service gateways or base stations have the capability to direct traffic from devices

that are not fully activated or provisioned to an Internet destination, or if the service processor 115 is used for such direction. In some embodiments, the activation server 160 is included in the service controller 122.

[0113] FIG. 2 illustrates another simplified (e.g., “flattened”) network architecture including an MVNO (Mobile Virtual Network Operator) relationship in accordance with some embodiments. As shown, an open MVNO configuration is provided in a simplified network as similarly described above with respect to FIG. 1. In some embodiments, the service provider (e.g., service owner) is defined by the entity that maintains and/or manages the service controller 122 associated with and controlling the service processors 115 that are inside the devices 100 using the service. In some embodiments, the service controller 122 requires only a non-real time relatively low data rate secure control plane communication link to the service processors 115. Accordingly, in some embodiments, the service controller 122 servers can reside in any network that can connect to (e.g., be in network communication with) the Internet 120. For example, this approach provides for a more efficient provisioning of the equipment used to set up an MVNO partnership between the central provider and the service provider, and as shown in FIG. 2, an MVNO network 210 is in network communication with the Internet 120 just as with the central provider network 110 is in network communication with the Internet 120. As shown, the following are connected to (e.g., in network communication with) the MVNO core network 210: MVNO billing system 123, MVNO service controller 122, MVNO content management system 130, MVNO DNS/DHCP server 126, MVNO AAA server 121, and MVNO mobile wireless center 132.

[0114] By showing two service controllers 122, one connected to (e.g., in network communication with) the MVNO network 210 and one connected to the central provider network 110, FIG. 2 also illustrates that some embodiments allow two entities on the same access network to each use the service controller 122 and service processor 115 to control different devices and offer different or similar services. As described below, the unique secure communication link pairing that exists between the two ends of the service control link, 1691 and 1638 (as shown in FIG. 16), ensure that the two service controllers 122 can only control the devices associated with the correct service provider service profiles.

[0115] FIG. 3 illustrates another simplified (e.g., “flattened”) network architecture including two central providers in accordance with some embodiments. For example, this provides for roaming agreements while maintaining rich services across different networks with completely different access layers. As shown, the mobile devices 100 are assumed to have a dual mode wireless modem that will operate on both a 4G network, for example LTE or WiMax, and a 3G network, for example HSPA or EVDO. One example roaming condition would be both Central Provider #1 and Central Provider #2 providing 3G and 4G network resources. In this example, the mobile devices 100 can connect to both 3G and 4G base stations 125 owned and operated by the central provider with whom they have signed up for service, or when neither is available from the central provider the user signed up with the device can roam onto the other central provider access network and still potentially offer the same rich service set using the same service profiles provided, for example, the roaming service costs are reasonable. In some embodiments, if roaming service costs are significantly more expensive than home network service costs, then the service processor 115 is configured with a roaming service profile that reduces or tailors service usage or service activity through a combination of one or more of user notification, user preference feedback regarding traffic shaping or service policy management preference collected and acted on by service processor 115, adaptive policy control in service processor 115 that tracks increasing roaming service costs and scales back service, or recognition of the change in network that causes the service controller 122 to configure service processor 115 of device 100 with a roaming service profile. In some embodiments, in roaming situations, network selection can be based on an automatic network selection with network selection being determined, for example, by a combination of user service profile preferences, service provider roaming deals and/or available roaming network capabilities and cost, as discussed further below.

[0116] In some embodiments, the devices 100 are again assumed to be multimode 3G and 4G devices (e.g., the mobile devices 100 are assumed to have a dual mode wireless modem that will operate on both a 4G network, for example LTE, and a 3G network, for example HSPA or EVDO), with the devices 100 being billed for service by Central Provider #1 being, for example, EVDO and LTE capable, and the devices 100 being billed for service by Central Provider #2 being, for example, HSPA and LTE capable. For example, the devices 100 can roam using the 4G LTE network of the roaming central provider when neither the 3G nor 4G

networks are available with the home central provider. As similarly discussed above with respect to the above described roaming embodiments, the service processors 115 and service controllers 122 are capable of providing similar services on the 4G roaming network and the 3G home network as on the 4G home network, however, the varying costs and available network capacity and speed differences of 3G home, 4G roaming and 4G home may also encourage the use of different, such as three different, service profiles to allow for the most effective and efficient selection and control of services based on the current network.

[0117] FIG. 4 illustrates a network architecture including a Universal Mobile Telecommunications System (UMTS) overlay configuration in accordance with some embodiments. As shown, FIG. 4 includes a 4G/3G/2G HSPA/Transport access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. In some embodiments, the central provider can offer improved service capabilities using a conventional UMTS network. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the conventional UMTS network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled across the various UMTS network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121. Referring now to the 4G/3G/2G HSPA/Transport access network as shown in FIG. 4, the LTE/HSPA and HSPA/GPRS base stations/nodes 125 are in communication with 4G/3G/2G Service/Serving GPRS Support Nodes (SGSNs) cluster 410 via a radio access network 405, which are in communication with 4G/3G/2G Gateway GPRS Support Nodes (GGSNs) cluster 420 via an access transport network 415 (e.g., a GPRS-IP network), which are then in communication with central provider core network 110.

[0118] As shown in FIG. 4, as discussed elsewhere, service usage data store 118 is a functional descriptor for a network level service usage information collection and reporting function located in one or more of the networking equipment boxes attached to one or more of the sub-networks in the figure (e.g., RAN, transport and/or core networks). As shown in FIG. 4, service usage 118 is shown as an isolated function connected to the central provider core network 110 and the intention of this depiction is to facilitate all the possible embodiments for

locating the service usage 118 function. In some UMTS network embodiments, the service usage 118 function is located or partially located in the GGSN gateway (or gateway cluster) 420. In some embodiments, service usage 118 functionality is located or partially located in the SGSN gateway (or gateway cluster) 410. In some embodiments, service usage 118 functionality is located or partially located in the equipment cluster that includes the AAA 121 and/or the mobile wireless center 132. In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station 125 in FIG. 4 and many other figures described herein. In some embodiments, service usage 118 functionality is located or partially located in a networking component in the transport network 415, a networking component in the core network 110, the billing system 123 and/or in another network component or function. This discussion on the possible locations for the network based service usage history logging and reporting function can be easily generalized to all the other figures described herein by one of ordinary skill in the art (e.g., RAN Gateway 410 and/or Transport Gateway 420), and this background will be assumed even if not directly stated in all discussion above and below.

[0119] In some embodiments, a central provider provides open development services to MVNO, Master Value Added Reseller (MVAR) and/or Original Equipment Manufacturer (OEM) partners. In some embodiments, all three service providers, central provider service provider, MVNO #1 service provider and MVNO #2 service provider have service control and billing control of their own respective devices 100 through the unique pairing of the service processors 115 and service controllers 122. For example, MVNO #1 and MVNO #2 can each have open development billing agreements with the central provider and each can own their respective billing systems 123. As shown in FIG. 4, MVNO #1 core network 210 is in communication with the central provider core network 110 via the Internet 120, and MVNO #2 core network 210 is in communication with the central provider core network 110 via an alternate landline(LL)/VPN connection 425. In some embodiments, the two MVNOs each offer completely different devices and/or services, and the devices and/or services also differ significantly from those offered by the central provider, and the service profiles are adapted as required to service the different devices and respective service offerings. In addition, the central billing system 123 allows all three service provider user populations to access ecommerce experiences from transaction provider partners operating transaction servers 134, to choose

central provider billing options that combine their third party transaction bills on their service provider bill, and each subscriber population can experience a service provider specified look and feel that is unique to the respective service provider even though the different user populations are interfacing to the same transaction servers and the transaction partners do not need to require significant custom development to provide the unique central billing and unique consistent user experience look and feel.

[0120] In some embodiments, a central provider offers open network device and service developer services using one service controller server 122 (e.g., a service controller server farm) and allows the open development partners to lease server time and server tools to build their own service profiles. The central provider also provides service billing on behalf of services to the open development partners. For example, this reduces costs associated with setting up an MVNO network for the open development partners and does not require the partners to give up significant control or flexibility in device and/or service control.

[0121] FIG. 5 illustrates a network architecture including an Evolution Data Optimized (EVDO) overlay configuration in accordance with some embodiments. This figure is similar to FIG. 4 except for the various particular variations of the EVDO network architecture as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill in the art. As shown, FIG. 5 includes an EVDO access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. The EVDO access network includes LTE/EVDO and EVDO/1xRTT base stations 125 in communication with Base Station Controller (BSC) packet control 508 and radio network controller 512 via a radio access network (RAN) 505, which are in communication with packet data service node 520 via an access transport network 515, which is in communication with central provider core network 110. As shown, a RAN AAA server 521 is also in communication with the access transport network 515.

[0122] In some embodiments, the central provider can offer improved service capabilities using a wireless access network. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure

control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

[0123] FIG. 6 illustrates a network architecture including a 4G LTE and Wi-Fi overlay configuration in accordance with some embodiments. This figure is also similar to FIG. 4 except for the various particular variations of the 4G LTE/Wi-Fi network architecture as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill. As shown, FIG. 6 includes a 4G LTE and Wi-Fi access network operated by a central provider and two MVNO networks 210 operated by two MVNO partners. The 4G LTE/Wi-Fi access network as shown includes LTE eNodeB and HSPA/EVDO base stations 125 in communication with Base Station Controller (BSC) packet control (EVDO & 1xRTT) 608 and SGSN (HSPA & GPRS) 612 via a radio access network (RAN) 605, which are in communication with System Architecture Evolution (SAE) Gateway (GW) 620 via an access transport network 615, which is then in communication with central provider (core) network 110. As shown, a Mobile Management Entity (MME) server 619 is also in communication with the access transport network 615. Also as shown, a Wi-Fi Access Point (AP) 602 is also in communication with the access transport network 615 via Wi-Fi Access Customer Premises Equipment (CPE) 604. As will be apparent to those of ordinary skill in the art, the embodiments of network architectures shown, for example, in FIGS. 1-8 are exemplary network architecture embodiments in which one or more of the shown network elements may not be required or included, alternative network elements included, and/or additional network elements included based on network design choices, network standards and/or other functional/design considerations and choices.

[0124] In some embodiments, the central provider can offer improved service capabilities using the wireless access network as depicted in FIG. 6. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

Accordingly, as shown in FIGS. 4 through 6, various embodiments can be implemented independent of the wireless access network technology, and for example, can be implemented in 3G, 4G and any other wireless access network technology.

[0125] FIG. 7 illustrates a network architecture including a WiMax and Wi-Fi overlay configuration in accordance with some embodiments. This figure is also similar to FIG. 4 except for the various particular variations of a combined WiMax/Wi-Fi network as compared to the HSPA/GPRS wireless access network architecture as will be apparent to one of ordinary skill in the art. As shown, FIG. 7 includes both a WiMax and Wi-Fi network (e.g., a combined WiMax/Wi-Fi network) operated by a central provider and two MVNO networks 210 operated by two MVNO partners. Although the Wi-Fi and WiMax access technologies are different wireless access networking technologies, with WiMax providing a wide area networking technology and Wi-Fi providing a local area networking technology, which efficiently operates using the two wireless access networking capabilities. As similarly discussed above with respect to the switching between 3G and 4G networks, some embodiments employ the automatic network selection capability as described above to choose the best available network service profile, and, for example, the user can force the decision or the service controller can make the decision. For example, if free Wi-Fi services have adequate coverage, in most cases, the decision criteria programmed into the automatic network selection algorithm will select Wi-Fi as long as the Wi-Fi access points are associated with a known and trusted provider. In some embodiments, transaction billing from central provider billing system 123 or MVNO #1 or MVNO #2 billing systems 123 will work with the transaction servers when connected over Wi-Fi just as when connected over any other access technology (including wire line based connections). The WiMax/Wi-Fi access network as shown includes WiMax base stations 125, Wi-Fi access points/hotspots 702 and/or Wi-Fi mesh access networks 702 (in some embodiments, femto cells can be used in addition to and/or as an alternative to Wi-Fi), and Wi-Fi access customer-premises equipment (CPE) 704 in communication with WiMax service controller 708 and Wi-Fi service controller 712 via a radio access network 705, which are in communication with WiMax core gateway 720 via an access transport network 715, which is then in communication with central provider (core) network 110.

[0126] In some embodiments, the central provider can offer improved service capabilities using the wireless access network as depicted in FIG. 7. As shown, the base stations 125 do not connect directly to the Internet 120, and instead the base stations 125 connect to the wireless access network. However, as in various previous embodiments, the service processor 115 still connects through the secure control plane link to service controller 122. In some embodiments, the data plane traffic is backhauled as shown across the various network routers and gateways as is the control plane traffic, and the IPDRs are obtained from the access network AAA server 121.

[0127] Referring to FIG. 7, the Wi-Fi connection can be replaced with a femto cell (and the Wi-Fi modem shown in FIGS. 15D and 15E can be replaced with a femto cell modem (base station side functionality)). In some embodiments, the service processor 115 is provided on the femto cell to control subscriber access in a verifiable manner as similarly described herein with respect to various embodiments (e.g., the Wi-Fi related embodiments). For example, the femto cell service provider (e.g., the entity that owns the spectrum the femto cell is using) can operate the femto cell as a local access mechanism for the home subscriber (or other who purchased or installed the femto cell), and then also use it to provide pay-for-service or additional free services, with controlled access and/or traffic control and/or service control and/or billing control performed locally or in combination with network equipment as described herein. In some embodiments, the WWAN devices being used at home or work with the femto cell include a portion of the service processor functionality. For example, this allows the service provider for femto cells to provide service and monetize service in a controlled way even though the femto cell is not connected to the service provider network the way conventional base stations are connected to the service provider network, but is connected through the Internet 120. For example, the secure heartbeat function can be extended to include data traffic so that it is encrypted and secured along with the control plane traffic. The decision of whether or not to admit a device onto the femto cell can be made through the service processor 115 connection to the service controller 122 and subsequent look up of the credentials for the device and the associated service plan and service profile that is then programmed into the service processor on the femto cell and/or the device itself. The femto cell can also offer a landing page to devices through the service processor so that devices that do not belong to the network can gain access to the network by signing up over the femto cell. For example, the intermediate device embodiments for Wi-Fi on one end and WWAN on the other can be accomplished by using the

Wi-Fi connection in the cell phone in AP mode so that it becomes the intermediate device. The service processor 115 on the cell phone can then act in the same manner as described for the intermediate device as described herein.

[0128] FIG. 8 illustrates another simplified (e.g., “flattened”) network architecture including multiple wireless access networks (e.g., 3G and 4G Wireless Wide Area Networks (WWANs)) and multiple wire line networks (e.g., Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks) in accordance with some embodiments. It is a common network architecture for multi-access central providers to have one or more wired access networks and one or more wireless access networks. As shown, FIG. 8 includes both 3G and 4G wireless access networks, including a 4G base station 125 and a 3G base station 125, and both DOCSIS and DSLAM wire line networks (e.g., a combined WWAN/wire line network), including DOCSIS Head End 125 and DSLAM 125, operated by a central provider via central provider (core) network 110 and an MVNO partner via MVNO network 210 via the Internet 120.

[0129] As shown, the service processor 115 can reside on a number of different types of devices 100 that work on 3G or 4G wireless, DSL or DOCSIS, and the service controller 122 is capable of controlling each of these types of devices with a consistent service experience, for example, using different service profiles, service capabilities and service profile cost options depending on which network the device is connected to and/or other criteria. For example, a download of a High Definition (HD) movie can be allowed when the service controller 122 is managing service profile policies for a service processor 115 residing on a DOCSIS device 100 (e.g., a computer or laptop connected to a cable modem), but not when the same service controller 122 is managing service profile policies for a service processor 115 residing on a 3G device 100 (e.g., a smart phone connected to a mobile 3G network).

[0130] As will now be apparent to one of ordinary skill in the art in view of the above description of FIGS. 1 through 8, the present invention can be provided across any access network and a set of service profiles can be defined in a variety of ways including, for example, to user preference feedback, access network performance, access network cost, access network central provider partnership status with the service provider central provider and roaming deals

and costs. For example, as discussed below, various embodiments allow for users to have superior service experiences based on the ability to control certain of their service settings, and service providers can also more efficiently deploy a greater variety of services/service plans to users.

[0131] In some embodiments, the service processor 115 and the service controller 122 provide an overlay for existing networks without significantly changing the billing system 123, gateways/routers or other network components/elements, and also provide verifiable service monitoring to control services and/or service usage/costs without involving, for example, a service provider or MVNO (e.g., for smart phone devices and/or laptops or netbooks (or any other network accessible device) with an unlimited data plan or any other service plan). For example, applications that are deployed by device owners or service subscribers (e.g., an IT manager) and do not involve a service provider include roaming services provided as an after-market product without carrier/service provider involvement. In this example, device activity is recorded by the service processor 115 and transmitted to the service controller 122 (e.g., the IT manager controls the service controller 122). In another example, a third party after-market product is provided in which the service controller 122 is hosted by the third party and the device management entity (e.g., the IT manager or parents of the device user for parental controls) uses a secure Virtual Service Provider (VSP) website to control the devices that belong to that management entity's device partition (e.g., VSP partitions and techniques are described below with respect to FIG. 49). The VSP secure website techniques described herein can also be applied to service provider owned servers with device partitions for the purpose of controlling, for example, Deep Packet Inspection (DPI) controllers (e.g., DPC policy implementation 5402 as shown in FIG. 54) to provide similar or substantially equivalent service usage/control capabilities using network based service control techniques, as similarly described in detail below with respect to FIGS. 49 and 54 (e.g., IT manager VSP control of a group partition and/or MVNO VSP control of a group partition).

Service Processor Configurations for Devices

[0132] FIG. 9 illustrates a hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 9, the service processor

115 is stored in a non volatile memory 910 and a memory 920 of the device 100. As will be appreciated by those of ordinary skill in the art, the present invention can operate with virtually any device architecture, and the device architectures discussed herein (e.g., with respect to FIGS. 9-14 and 15A-15F) are examples of various implementations on certain devices (e.g., of different representations of device 100).

[0133] As shown in FIG. 9, device 100 also includes a processor 930, sometimes referred to as a CPU or central processor unit, an APU or application processor unit, a core processor, a computing device, or many other well known terms. In some embodiments, device 100 includes one or more processors and/or a multicore processor. As shown, processor 930 includes a sub-processor 935. In some embodiments, processor 930 and/or sub-processor 935 are based on an architecture sometimes referred to as a complex instruction set computer or CISC, a reduced instruction set computer or RISC, a parallel processor, a combination of two or more architectures or any other processor architecture. In some embodiments, processor 930 has a design that is based on logic and circuitry from one or more standard design library or published architecture, or includes specialized logic and circuitry designed for a given device 100 or collection of such devices. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, one processor and/or sub-processor can have one architecture while another may have a somewhat different or completely different architecture. In some embodiments, one or more of the processors and/or sub-processors can have a general purpose architecture or instruction set, can have an architecture or instruction set that is partially general or partially specialized, or can have an instruction set or architecture that is entirely specialized. In some embodiments, a device includes more than one processor and/or sub-processor, and in such a device, there can be a division of the functionality for one or more processors and/or sub-processors. For example, one or more processors and/or sub-processors can perform general operating system or application program execution functions, while one or more others can perform communication modem functions, input/output functions, user interface functions, graphics or multimedia functions, communication stack functions, security functions, memory management or direct memory access functions, computing functions, and/or can share in these or other specialized or partially specialized functions. In some embodiments, any processor 930 and/or any sub-processor 935 can run a low level operating system, a high level operating system, a combination of low level and high level operating systems, or can include

logic implemented in hardware and/or software that does not depend on the divisions of functionality or hierarchy of processing functionality common to operating systems.

[0134] As shown in FIG. 9, device 100 also includes non-volatile memory 910, memory 920, graphics memory 950 and/or other memory used for general and/or specialized purposes. As shown, device 100 also includes a graphics processor 938 (e.g., for graphics processing functions). In some embodiments, graphics processing functions are performed by processor 930 and/or sub-processor 935, and a separate graphics process 938 is not included in device 100. As shown in FIG. 9, device 100 includes the following modems: wire line modem 940, WWAN modem 942, USB modem 944, Wi-Fi modem 946, Bluetooth modem 948, and Ethernet modem 949. In some embodiments, device 100 includes one or more of these modems and/or other modems (e.g., for other networking/access technologies). In some embodiments, some or all of the functions performed by one or more of these modems are performed by the processor 930 and/or sub processor 935. For example, processor 930 can implement some or all of certain WWAN functional aspects, such as the modem management, modem physical layer and/or MAC layer DSP, modem I/O, modem radio circuit interface, or other aspects of modem operation. In some embodiments, processor 930 as functionality discussed above is provided in a separate specialized processor as similarly shown with respect to the graphics and/or multimedia processor 938.

[0135] As also shown in FIG. 9, device 100 includes an internal (or external) communication bus structure 960. The internal communication bus structure 960 generally connects the components in the device 100 to one another (e.g., allows for intercommunication). In some embodiments, the internal communication bus structure 960 is based on one or more general purpose buses, such as AMBA, AHP, USB, PCIe, GPIO, UART, SPI, I²C, Fire wire, DisplayPort, Ethernet, Wi-Fi, Bluetooth, Zigbee, IRDA, and/or any other bus and/or I/O standards (open or proprietary). In some embodiments, the bus structure is constructed with one or more custom serial or parallel interconnect logic or protocol schemes. As will be apparent to one of ordinary skill in the art, any of these or other bus schemes can be used in isolation and/or in combination for various interconnections between device 100 components.

[0136] In some embodiments, all or a portion of the service processor 115 functions disclosed herein are implemented in software. In some embodiments, all or a portion of the service processor 115 functions are implemented in hardware. In some embodiments, all or substantially all of the service processor 115 functionality (as discussed herein) is implemented and stored in software that can be performed on (e.g., executed by) various components in device 100. FIG. 9 illustrates an embodiment in which service processor 115 is stored in device memory, as shown, in memory 920 and/or non-volatile memory 910, or a combination of both. In some embodiments, it is advantageous to store or implement certain portions or all of service processor 115 in protected or secure memory so that other undesired programs (and/or unauthorized users) have difficulty accessing the functions or software in service processor 115. In some embodiments, service processor 115, at least in part, is implemented in and/or stored on secure non-volatile memory (e.g., non volatile memory 930 can be secure non-volatile memory) that is not accessible without pass keys and/or other security mechanisms. In some embodiments, the ability to load at least a portion of service processor 115 software into protected non-volatile memory also requires a secure key and/or signature and/or requires that the service processor 115 software components being loaded into non-volatile memory are also securely encrypted and appropriately signed by an authority that is trusted by a secure software downloader function, such as service downloader 1663 as discussed below (and as shown in FIG. 16). In some embodiments, a secure software download embodiment also uses a secure non-volatile memory. Those of ordinary skill in the art will also appreciate that all memory can be on-chip, off-chip, on-board and/or off-board. In some embodiments, the service processor 115 which as shown in FIG. 9 is stored or implemented in non volatile memory 910 and memory 920, can be implemented in part on other components in device 100.

[0137] As shown, device 100 also includes a user interfaces device component 980 for communicating with user interface devices (e.g., keyboards, displays and/or other interface devices) and other I/O devices component 985 for communicating with other I/O devices. User interface devices, such as keyboards, display screens, touch screens, specialized buttons or switches, speakers, and/or other user interface devices provide various interfaces for allowing one or more users to use the device 100.

[0138] FIG. 10 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 10, the service processor 115 is implemented on the processor 930 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the processor 930. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the processor 930. While the service processor 115 is shown in FIG. 10 as stored, implemented and/or executed on the processor 930, in other embodiments, the service processor 115 is implemented in part on other components in device 100, for example, as discussed below.

Service Processor Implemented on a Communications Modem

[0139] FIG. 11 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 11, the service processor 115 is implemented on the WWAN modem 942 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the WWAN modem 942. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the WWAN modem 942. In some embodiments, service process 115 is implemented on another modem component of device 100 and/or one or more of the modem components of device 100.

[0140] In some embodiments, the service processor 115 is implemented on a modem processor (e.g., WWAN modem 942 or WWAN/Wi-Fi modem), and the service processor 115 can be installed and/or executed in protected and/or secure memory or processor hardware on the modem. The modem memory can be made robust to hacking or tampering and, in some embodiments, is only accessible from a secure network management channel or secure device management port and not by most end users. In some embodiments, a portion of the service processor 115 is implemented on a modem processor (e.g., WWAN modem 942 hardware or software), and a portion of the service processor 115 is implemented on another device 100 processor 930. For example, the device service monitor agent 1696 and one or more service usage measurement points (see discussion associated with FIG. 21) can be implemented on a modem processor, and other service processor 115 elements can be implemented in the main

device operating system processor 930. As another example, a second (or first) service monitor agent 1696 and one or more service usage measurement points can be implemented on a modem processor, and a first (or second) service monitor 1696 with one or more service measurement points can be implemented on the main operating system processor 930 for device 100. For example, such embodiments can be configured to provide a service usage measurement and reporting system that offers a diversified countermeasure to protect against hacking, tampering or other errors for device based service usage measurements that can be made harder to hack or tamper with than certain software embodiments on the processor 930. For example, such embodiments can be employed when one or more of the following capabilities are not available: network based service usage measures, network based service profile or policy implementation verification measures, and network based service usage verification error response action capabilities.

[0141] In some embodiments, certain portions of the service processor 115 that deal with application layer service monitoring or traffic flow identification (e.g., tagging or traffic flow shaping as disclosed elsewhere) are implemented on a main processor 930, and other portions of the service processor 115 are implemented on a modem processor (e.g., WWAN modem 942).

[0142] In some embodiments, the WWAN modem is a wide area access technology modem such as 2G, 2.5G, 3G or 4G. As discussed above and below, the connection to the WWAN modem 942 can be a connection internal to device 100, for example a USB, GPIO, AMBA or other bus, or can be a connection that extends external to the device such as for example a USB, Ethernet, Wi-Fi, Bluetooth or other LAN or PAN connection. Three example embodiments in which the bus is internal to the device are as follows: a PCIe modem card running over USB or PCIe, a GPIO connection running from a processor 930 chipset to a modem chipset inside a mobile device, or a Wi-Fi connection running from a Wi-Fi modem inside of device 100 to an intermediate modem or networking device combination that forwards the access network traffic between the access network connection and the device via the Wi-Fi connection. In some embodiments, in addition to the service processor 115 being implemented on the WWAN modem 942 either internal or external to the device 100, similarly service processor 115 can be implemented on a wire line modem 940, such as DSL, Cable or fiber, another wireless LAN or PAN modem, such as Wi-Fi, Zigbee, Bluetooth modem 948, White Space, or some other

modem, connected internal to device 100 or external to device 100 via a LAN or PAN extension of internal or external communications bus structure 960.

[0143] In some embodiments, a complete turn-key reference design product for the device modem (one or more of 942, 946, 948, 949, 944, 940) combined with a built-in service processor 115, possibly with a well defined and documented application interface and a well defined and documented service processor developers kit (SPDK) provides for a powerful product embodiment for the purpose of achieving mass market distribution and usage for the modem with service processor 115 and associated service controller 122 features. For example, embodiments that include the WWAN modem 942, possibly in combination with one or more additional modems including Wi-Fi modem 946, bluetooth modem 948, USB modem 944 and Ethernet modem 949, can be combined with a pre-tested or pre-certified integrated embodiment of the service processor 115, possibly in combination with a well defined API for writing software applications that interface to, reside on or communicate with this turn-key modem embodiment. As disclosed herein, the advantageous capabilities of the service processor 115, possibly in conjunction with the service controller 122, to assist in monitoring, control, billing and verification for services is made more available for device 100 manufacturers in such a form, because the manufacturers do not need to spend as much time and resources to develop a custom modem only for a subset of devices that the turn-key modem can be used to support. In some embodiments, the service processor 115, as discussed herein, can be configured to provide device assisted service monitoring, control, billing and/or verification across not just when connected to the WWAN network via the WWAN modem, but also when connected to the other networks corresponding to the other access modems included in the turn-key combined module plus service processor 115 (or SPDK or chipset plus service processor 115) design. The pre-integrated service processor 115 and API possibly in combination with testing and certification can be packaged in a small form factor that may have standardized interfaces such as USB, PCIe, firewire, Display Port, GPIO, or other interface. The form factor may be miniaturized into standard configurations such as minicard, half minicard or even smaller form factors, or it can be designed into a non-standard or proprietary form factor. The module form factor can be well documented to simplify integration into various device 100 designs. The SPDK embodiments can be designed to contain one or more of the following: hardware integration and use documentation, software integration documentation, software programming documentation,

application interface documentation, service controller documentation, overall testing guidelines and overall use guidelines. In some embodiments, the modem module can be integrated with the service processor 115 functionality as a combined chipset, firmware and/or software product, with other SPDK features very similar to those listed above. The service controller programming guide for these turn-key embodiments can also be documented for the SPDK service processor 115 software, turn-key module with service processor 115 or integrated chipset with service processor 115. Accordingly, these embodiments provide various solutions to simplify the OEM task of integrating, developing, testing and shipping device 100 products (or integrated networking device products) with any of the device assisted service monitoring, control, billing or verification capabilities disclosed herein.

[0144] FIG. 12 illustrates another hardware diagram of a device 100 that includes a service processor 115 in accordance with some embodiments. As shown in FIG. 12, the service processor 115 is implemented on the other I/O devices component 980 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the other I/O devices component 980 (e.g., a SIM/USIM card or other secure hardware I/O device). In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the other I/O devices component 980.

[0145] As discussed above, various embodiments include product designs in which the service processor 115 resides on device volatile or non-volatile memory (see FIG. 9), the device application processor or CPU (see FIG. 10), the wireless access modem (see FIG. 11) (or any other modem), or another I/O device (see FIG. 12). While these are just a few of the example service processor 115 placement embodiments, these embodiments show that the placement of where the software or hardware for implementing the service processor 115 can reside in the device 100 is very flexible and can be implemented in a myriad of places and ways depending on the device and/or other technical design choices.

[0146] FIG. 13 illustrates another hardware diagram of a device 100 that includes a service processor 115 implemented in external memory of a System On Chip (SOC) 1310 in accordance with some embodiments. As shown in FIG. 13, the service processor 115 is

implemented on the external memory 1320 of the device 100. In some embodiments, this implementation can be in part or whole accomplished in software stored, implemented and/or executed on the external memory 1320. In some embodiments, the implementation and/or execution can be in part or whole accomplished in hardware that is on the external memory 1320. In some embodiments, SOC chipset 1310 and external memory 1320 provide a portion or all of the hardware of device 100.

[0147] FIG. 14 illustrates another hardware diagram of a device 100 that includes a service processor 115 implemented in external memory of a System On Chip (SOC) 1310 in accordance with some embodiments. As shown, the service processor 115 is stored in a non volatile memory 910 and a memory 920 of the SOC chipset 1310, as similarly discussed above with respect to FIG. 9. In some embodiments, SOC chipset 1310 and external memory 1320 provide a portion or all of the hardware of device 100.

[0148] As similarly discussed above with respect to FIGS. 9 through 12, various embodiments include product designs including the SOC chipset 1310 in which the service processor 115 resides on internal volatile or non-volatile memory 910 of the SOC chipset 1310 (see FIG. 14), the device application processor or CPU 930 and/or sub processor 935, the modems 940, 942, 944, 946, 948, and/or 949 (or any other modem), another I/O device 985, and/or external memory 1320 (see FIG. 13) (and/or any combinations thereof). While these are just a few of the example service processor 115 placement embodiments, these embodiments show that the placement of where the software or hardware for implementing the service processor 115 can reside in the SOC chipset 1310 and/or the external memory 1320 of the device 100 is very flexible and can be implemented in a myriad of places and ways depending on the device and/or other technical design choices.

[0149] The above discussion with respect to FIGS. 9 through 14 illustrating various internal hardware embodiments for device 100 applies equally to this partitioning of device functionality or any other partitioning of how the components in device 100 are configured, whether they are all separate components, some of the components are combined into a single chipset but there are still multiple chipsets, or all of the components are combined into a chipset. For example, FIGS. 9 through 14 illustrating various internal hardware embodiments for device

100 show several access modem components including the wire line modem 940, wireless wide area network (WWAN) modem 942, USB modem 944, Wi-Fi modem 946, Bluetooth modem 948, and Ethernet modem 949. In some embodiments, wire line modem 940 is a DSL or cable modem such as DOCSIS, or some other modem with a hard connection such as fiber. In some embodiments, as discussed above and below, connection to the wire line or wireless access network is accomplished through an extension of the internal or external communications bus structure 960. For example, such an extension is accomplished using one or the other modems, such as Wi-Fi modem 946 or Ethernet modem 949, connecting to a local area network that in turn connects to the access network via a device that bridges the local area network to the access network. One of ordinary skill in the art will appreciate that when discussing device connection to any access network the connection can be via a direct connection to the network, such as a 3G or 4G WWAN modem 942 connection to a 3G or 4G WWAN network, or can be a connection to the access network through an intermediate connection, such as a Wi-Fi modem 946 connection to a modem or networking device combination that has a Wi-Fi LAN connection and a 3G or 4G network access network connection. Another example of an extended modem connection embodiment includes a Wi-Fi modem 946 device connection to a modem or networking device combination that includes a Wi-Fi LAN connection and a DOCSIS or DSL network access connection. Other examples of such combinations will be readily apparent to one of ordinary skill in the art.

Service Processor Configurations for Intermediate Networking Devices

[0150] FIGS. 15A through 15F illustrate hardware diagrams of a device 100 that include a service processor 115 and a bus structure extension 1510 using intermediate modem or networking device combinations in accordance with various embodiments. For example, FIGS. 15A through 15E illustrate various extended modem alternatives for access network connection through an intermediate modem or networking device combination that has a connection (e.g., LAN connection) to one or more devices 100.

[0151] In some embodiments, device 100 includes a 3G and/or 4G network access connection in combination with the Wi-Fi LAN connection to the device 100. For example, the intermediate device or networking device combination can be a device that simply translates the

Wi-Fi data to the WWAN access network without implementing any portion of the service processor 115 as shown in FIG. 15B. In some embodiments, an intermediate device or networking device combination includes a more sophisticated implementation including a networking stack and some embodiments a processor, as is the case for example if the intermediate networking device or networking device combination includes a router function, in which case the service processor 115 can be implemented in part or entirely on the intermediate modem or networking device combination. The intermediate modem or networking device combination can also be a multi-user device in which more than one user is gaining access to the 3G or 4G access network via the Wi-Fi LAN connection. In the case of such a multi-user network, the access network connection can include several managed service links using multiple instantiations of service processor 115, each instantiation, for example, being implemented in whole or in part on device 100 with the intermediate modem or networking device combination only providing the translation services from the Wi-Fi LAN to the WWAN access network.

[0152] Referring now to FIGS. 15A, 15C, 15D, and 15E, in some embodiments, the service processors 115 are implemented in part or in whole on the intermediate modem or networking device combination. In the case where the service processor 115 is implemented in part or in whole on the intermediate modem or networking device combination, the service processor 115 can be implemented for each device or each user in the network so that there are multiple managed service provider accounts all gaining access through the same intermediate modem or networking device combination. In some embodiments, the functions of service processor 115 are implemented on an aggregate account that includes the WWAN access network traffic for all of the users or devices connected to the Wi-Fi LAN serviced by the intermediate modem or networking device combination. In some embodiments, the central provider can also provide an aggregated account service plan, such as a family plan, a corporate user group plan and/or an instant hotspot plan. In the case where there is one account for the intermediate modem or networking device combination, the intermediate modem or networking device combination can implement a local division of services to one or more devices 100 or users in which the services are controlled or managed by the intermediate modem or networking device combination or the device 100, but the management is not subject to service provider control and is auxiliary to the service management or service policy implementation performed

by service processors 115. In some embodiments, another service model can also be supported in which there is an aggregate service provider plan associated with one intermediate modem or networking device combination, or a group of intermediate modems or networking device combinations but where each user or device still has its own service plan that is a sub-plan under the aggregate plan so that each user or device has independent service policy implementation with a unique instantiation of service processor 115 rather than aggregate service policy implementation across multiple users in the group with a single instantiation of service processor 115.

[0153] As shown in FIGS. 15A and 15C, in some embodiments, device 100 includes a Wi-Fi modem 946, a Wi-Fi modem 946 combined with a 3G and/or 4G WWAN modem 1530 on intermediate modem or networking device combination 1510, and the intermediate modem or networking device combination forwards WWAN access network traffic to and from device 100 via the Wi-Fi link. For example, the service processor 115 can be implemented in its entirety on device 100 and the service provider account can be associated exclusively with one device. This is an embodiment associated with one or more of FIGS. 29, 31, 32 or 34 discussed below, in which the modem bus represents the Wi-Fi LAN connection via the Wi-Fi modem 946. Similarly, as shown in FIGS. 15A and 15D, such an implementation can be provided using a different access modem and access network, such as a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use DSL as shown in FIGS. 15A and 15E, USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0154] In some embodiments, a portion of the service processor 115 is implemented on the device 100, such as the application interface agent 1693 and other supporting agents (see FIG. 16), and another portion of the service provider 115 is implemented on the intermediate modem or networking device combination, such as policy implementation agent 1690 or possibly modem firewall 1655 as well as other agents (see FIG. 16). This is an embodiment associated with one or more of FIGS. 30 or 36 discussed below, in which the modem bus in the figure represents the Wi-Fi LAN connection via the Wi-Fi modem 946. In this example, the

service provider 115 can still offer individual service plans associated exclusively with one device, or can offer an aggregate plan in which the portion of the service processor 115 located on the intermediate modem or networking device combination 1510 aggregates service plans into one WWAN connection but each individual device 100 has a unique service interface via the application interface agents and associated agents located on device 100. Similarly, such an implementation can be provided using a different access modem and access network, for example a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0155] In some embodiments, all of the service processor 115 is implemented on the intermediate modem or networking device combination 1510 and the aggregate device or user traffic demand from the LAN port is serviced through one service provider service plan account. This is an embodiment associated with FIG. 35 in which as discussed below the modem bus in the figure represents the Wi-Fi LAN connection via the Wi-Fi modem 946. Similarly, such an implementation can be provided using a different access modem and access network, for example a 2G and/or 3G WWAN, DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G and/or 4G access network connection to the intermediate modem or networking device combination 1510. In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0156] In some embodiments, the device 100 uses the on-board WWAN modem 942 when it is outside of Wi-Fi LAN coverage area for one or more trusted access networks for the device, and when the device comes within range of a Wi-Fi network associated with a intermediate modem or networking device combination connected to a trusted wire line access network, the device can switch to the Wi-Fi link service to connect service processor 115 to the trusted wire line access network. In some embodiments, the decision to switch to the Wi-Fi LAN associated with a trusted wire line access network can be made automatically by the device based on the policy implementation rules settings for the modem selection and control 1811

and/or the policy control agent 1692, can be made by the user, or can be made by the service controller 122 (see FIG. 18). In addition, various other embodiments similarly use USB, Ethernet, Bluetooth, or another LAN or point to point connection from device 100 to the intermediate modem or networking device combination 1510.

[0157] FIG. 15F illustrates another hardware diagram of a device 100 that includes a service processor 115 and a bus structure extension 1510 using intermediate modem or networking device combinations in accordance with various embodiments. In some embodiments, more than one access network connection is implemented in the intermediate modem or networking device combination 1510. This allows the device 100 to potentially connect through the intermediate modem or networking device combination with a choice of access network services. An example of such an embodiment is illustrated in FIG. 15F in which an access network router (e.g., an enterprise router) connected to a LAN with a wire line primary backhaul connection and a back up WWAN connection, for example 3G or 4G, to provide access services when the primary wire line connection fails. As discussed above, the service provider service profile for service processor 115 and the service plan account can be set up as an aggregate account with multiple users connected to the LAN. The service provider can elect to use an embodiment that includes a portion of the service processor 115 on each device 100 so that the account can be managed for each user or each device, or the service provider can elect to implement all of the necessary features in the service processor 115 on the intermediate modem or networking device combination so that there is no visibility to the individual devices 100 or users.

[0158] As described herein, various embodiments provide many service policy implementation options that can enhance the service provider control of the service experience and cost, or enhance the user control of the service experience and cost by providing a verifiable or compromise resistant solutions to manage service policy implementation on the intermediate modem or networking device combination, for one or both of the WWAN or wire line access networks, when the WWAN access network is active, or when the WWAN access network is inactive. The level of service control, user preference feedback and service policy implementation verification or compromise resistance enabled by these embodiments improves the offered back up services and primary wire line services. One of ordinary skill in the art will

also now appreciate that any number of wire line and/or wireless network access connections can be supported by the various embodiments as described herein, with any number of device architectures and architectures for intermediate modem or networking device combinations bridging the device to the access network of choice. Accordingly, various embodiments provide a verifiable managed service architecture, design and implementation for any number of single access and/or multi-access networks in which the service account can be consistent across multiple networks, and the service policies can be changed from network to network as deemed appropriate by the service provider with service notification, service cost control and privacy preference inputs from the user.

[0159] In various embodiments, the verification embodiments discussed herein for service policy implementation verification or service policy implementation compromise protection can be applied. In some embodiments, rather than attaching a service provider service plan account to a single device, it is attached to (e.g., associated with) a user. For example, when the user logs onto an access network with a service controller controlled by a service provider, regardless of what device the user logs onto with the user's service plan profile can be automatically looked up in the central billing system 123 and dynamically loaded (e.g., downloaded) onto the device 100 from the service controller 122 (e.g., a service profile provided on demand based on the user's identity). In some embodiments, in addition to dynamically loading the user's service policy implementation and control settings, one or more of the user's preferences including notification, service control, traffic monitor reporting privacy and Customer Relationship Management (CRM) reporting privacy are also dynamically loaded. For example, this allows the user to have the same service settings, performance and experience regardless of the device the user is logged into and using on the network. In addition, as discussed herein, in the various embodiments that call for roaming from one type of access network to another, the user service plan profile, that includes all of the above in addition to the service plan profile changes that take effect between different types of access network, can be used on any device and on any network, providing the user with a verifiable or compromise resistant, consistent service experience regardless of network or device.

[0160] Many of the embodiments described herein refer to a user using device 100. It is understood that there are also applications for these various embodiments that do not involve

user interfaces. Examples of such applications include equipment, apparatus or devices for automation, telemetry, sensors, security or surveillance, appliance control, remote machine to machine data connections, certain remote access configurations, two way power metering or control, asset tracking, people tracking or other applications in which a human user interface is not required for device 100.

[0161] Various embodiments of the device 100 described above include other I/O devices 985. In some embodiments, these other devices include other modems, other special purpose hardware components, and/or other I/O devices or drivers or modems to connect to other I/O devices. In some embodiments, these other devices include a Subscriber Identity Module (SIM) or Universal Subscriber Identity Module (USIM) device. In some embodiments, it is advantageous to implement some or all of the service processor 115 functions on an embodiment of device 100 that includes a SIM and/or a USIM. In some embodiments, the other I/O devices 985 include a hardware device designed to implement a portion or all of the service processor 115 functions. For example, this is advantageous in cases in which the original device 100 was not manufactured with the service processor 115; in cases in which dedicated hardware is desired to improve one or more aspects of service processor 115 performance; allowing users, for example, to have the same service settings, performance and experience regardless of the device the user is using on the network by using such a SIM and/or USIM (e.g., or implemented as a type of dongle); and/or in cases in which a separate component is desired to assist in compromise protection for one or more aspects of service processor 115.

[0162] As discussed above, some embodiments described herein provide for billing of certain access services. In some embodiments, various applications do not require or involve billing of certain services. For example, applications like enterprise IT (Information Technology) group management of enterprise workforce access policy implementation or access cost control or access security policy, privacy control, parental control, network quality of service control or enhancement, private network services, free access services, publicly funded access services, flat rate no-options service and other services, or other examples that will be apparent to one of ordinary skill in the art do not require billing functionality but benefit from many other aspects of various embodiments.

[0163] Service Processor and Service Controller for Verifiable Service Monitoring, Notification and Control

[0164] FIG. 16 is a functional diagram illustrating a device based service processor 115 and a service controller 122 in accordance with some embodiments. For example, this provides relatively full featured device based service processor implementation and service controller implementation. As shown, this corresponds to a networking configuration in which the service controller 122 is connected to the Internet 120 and not directly to the access network 1610. As shown, a data plane (e.g., service traffic plane) communication path is shown in solid line connections and control plane (e.g., service control plane) communication path is shown in dashed line connections. As previously discussed, it is understood that the division in functionality between one device agent and another is based on, for example, design choices, networking environments, devices and/or services/applications, and various different combinations can be used in various different implementations. For example, the functional lines can be re-drawn in any way that the product designers see fit. As shown, this includes certain divisions and functional breakouts for device agents as an illustrative implementation, although other, potentially more complex, embodiments can include different divisions and functional breakouts for device agent functionality specifications, for example, in order to manage development specification and testing complexity and workflow. In addition, the placement of the agents that operate, interact with or monitor the data path can be moved or re-ordered in various embodiments. For example, as discussed below in some embodiments, one or more of the policy implementation or service monitoring functions can be placed on one of the access modems located below the modem driver and modem bus in the communication stack as illustrated in certain figures and described herein. As discussed below, some simplified embodiment figures illustrate that not all the functions illustrated in all the figures are necessary for many designs, so a product/service designer can choose to implement those functions believed to be most advantageous or sufficient for the desired purposes and/or environment. The functional elements shown in FIG. 16 are described below.

[0165] As shown, service processor 115 includes a service control device link 1691. For example, as device based service control techniques involving supervision across a network become more sophisticated, it becomes increasingly important to have an efficient and flexible

control plane communication link between the device agents and the network elements communicating with, controlling, monitoring, or verifying service policy. In some embodiments, the service control device link 1691 provides the device side of a system for transmission and reception of service agent to/from network element functions. In some embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions. In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security or encryption are used to make the link robust to discovery, eavesdropping or compromise. In some embodiments, the service control device link 1691 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments disclosed herein for the service control device link 1691 provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements.

[0166] In some embodiments, the service control device link 1691 agent messages are transmitted asynchronously as they are generated by one or more of the service agents. In some embodiments, the service control device link 1691 performs collection or buffering of agent messages between transmissions. In some embodiments, the service control device link 1691 determines when to transmit based potentially on several parameters including, for example, one or more of the following parameters: periodic timer trigger, waiting until a certain amount of service usage or traffic usage has occurred, responding to a service controller message, responding to a service controller request, initiated by one or more agents, initiated by a verification error condition, initiated by some other error or status condition. In some embodiments, once a transmission trigger has occurred, the service control device link 1691 assembles all buffered agent communications and frames the communications.

[0167] In some embodiments, the transmission trigger is controlled by waiting for an amount of service usage, such as waiting until a certain amount of data traffic has passed, which reduces the control plane communication channel traffic usage to a fraction of the data plane traffic. For example, this approach preserves network capacity and reduces service cost even in traffic scenarios in which data traffic is light.

[0168] In some embodiments, the transmission trigger is based on waiting for an amount of service usage, and also including a minimum transmission rate that triggers a transmission according to one or more of the following parameters: a maximum time between transmissions clock to keep the service processor 115 in communication with the service controller 122 when little or no service usage is occurring, a polling request of some kind from the service controller 122, a response to a service controller heartbeat, a transmission generated by a service verification error event, or a transmission generated by some other asynchronous event with time critical service processor 115 (or service controller 122) messaging needs, such as a transaction or service billing event or a user request. For example, service control plane traffic down is reduced to a relatively inexpensive and capacity conserving trickle when device 100 data traffic is not significant. At the same time, this approach also provides an effective flow of real time or near real-time service control plane traffic that is both cost and capacity efficient, because the service control plane traffic is a relatively small percentage of the data plane traffic when data plane traffic usage is heavy. For example, when data plane traffic usage is heavy is generally the time when close monitoring of service policy implementation verification or compromise prevention can be particularly important and by keeping the control plane overhead to a fraction of data plane traffic close monitoring and control of services are maintained at a reasonable cost in terms of percentage of both bandwidth used and network capacity. In some embodiments, the service usage or service activity trigger occurs based on some other measure than traffic usage, such as a number of messages transacted, one or more billing events, number of files downloaded, number of applications run or time that an application has been running, usage of one or more specified applications, GPS coordinate changes, roaming event, an event related to another network connection to the device and/or other service related measures.

[0169] In some embodiments, the service control device link 1691 provides for securing, signing, encrypting or otherwise protecting communications before sending. For example, the service control device link 1691 can send to the transport layer or directly to the link layer for transmission. In some embodiments, the communications are further secured with transport layer encryption, such as TCP TLS (Transport Control Protocol Transport Layer Security) or another secure transport layer protocol. In some embodiments, communications are encrypted at the link layer, such as IPSEC (Internet Protocol Security), various VPN (Virtual Private

Network) services, other forms of IP layer encryption and/or another link layer encryption technique.

[0170] In some embodiments, the service control link 1691 includes the above discussed agent heartbeat function in which the agents provide certain required reports to the service controller 122 for the purpose of service policy implementation verification (e.g., verification related reports on certain aspects of the service processor 115) or for other purposes. For example, such agent heartbeat messages can be in the open/clear (unencrypted) or encrypted, signed and/or otherwise secured. In some embodiments, these messages include one or more of the below described types of messages: an agent information message, an agent check-in message and/or agent cross check message.

[0171] In some embodiments, an agent information message is included in the agent heartbeat service policy implementation verification message, which includes, for example, any information the agent needs to communicate to the service controller 122 as part of the operation of the service policy implementation system. For example, an agent response to a service controller challenge, as described below, can be included in the agent heartbeat service policy implementation verification message.

[0172] In some embodiments, an agent check-in message is included in an agent heartbeat service policy implementation verification message, which includes, for example, a transmission of a unique agent identifier, secure unique identifier, and/or hashed encrypted and signed message beginning with some shared secret or state variable for the hash. For example, an agent self-check can be included in the agent heartbeat service policy implementation verification message, which includes reporting on agent configuration, agent operation, agent code status, agent communication log, agent error flags, and/or other agent associated information potentially hashed, encrypted, signed or otherwise secured in the message (e.g., using a shared secret unique to that agent).

[0173] In some embodiments, an agent cross-check message is included in the agent heartbeat service policy implementation verification message, which includes, for example, reports on the status, configuration, operation observations, communication log or other aspects of another agent. For example, agent environment reports can be included in the agent heartbeat

service policy implementation verification message, which includes, for example, reports on certain aspects of the service processor 115 operating environment, such as software presence (e.g., installation status of certain operating system and/or application software and/or components thereof), observed communication with agents or communication attempts, memory accesses or access attempts, network accesses or access attempts, software downloads or attempted downloads, software removal or download blocking, service policy implementation verification or compromise event error conditions with respect to the operating environment for the service processor 115, and/or other messages regarding the verification or possibility of compromise associated with the service processor 115 operating environment or agents.

[0174] In some embodiments, the agent heartbeat function also provides regular updates for information important to user service notification services. For example, the network based elements can provide regular synchronization updates for the device based service usage or service activity counters in which service usage or service activity measures available from one or more network service history elements is transmitted to the device 100. This allows the service usage counter errors between the device service counter and the counters used for central billing to be minimized. A common service usage or service activity measure is total traffic usage measured to date within a time frame over which a service limit is applicable. Other service usage or service activity measures can also be tracked and reconciled in a similar manner.

[0175] In some embodiments for the heartbeat function, the service controller 122 verifies that the scheduled agent reports are being received and that the reports are within expected parameters. In some embodiments, the access control integrity server 1654 issues signed challenge/response sequences to the policy implementation agent 1690. For example, the challenges can be asynchronous, issued when an event or error condition occurs, issued on a schedule or issued when a certain amount of data has passed. This approach, for example, provides a second layer of service policy implementation verification that strengthens the service usage or service activity measurement verification. For example, a challenge/response can be sent over the heartbeat link for the purpose of verifying device agent integrity. Various challenge/response related verification embodiments are described below.

[0176] In some embodiments, the challenge/response heartbeat message can include sending any kind of command or query, secure or transmitted in the open, receiving a response from the agent and then evaluating the response to determine if the response is within a range of parameters expected for a correctly configured agent, an agent that is operating properly, an agent that is not partially compromised or an agent that is not entirely compromised. In some embodiments, the agent is only required to respond with a simple acknowledgement of the challenge. In some embodiments, the agent is required to respond with a message or piece of information that is known by the agent. In some embodiments, the agent is required to respond with a message or piece of information that is difficult for the agent to respond correctly with if it were to be partially or entirely compromised. In some embodiments, the agent is required to respond back with information regarding the operation or configuration of the agent that is difficult for the agent to respond properly with if the agent is not properly configured, not operating properly, is partially compromised or is entirely compromised. In some embodiments, the first agent is required to respond back with information regarding the operation, configuration, status or behavior of a second agent that is difficult for the first or second agent to respond properly with if the first or second agent is not properly configured, not operating properly, is partially compromised or is entirely compromised. In some embodiments, the agent is required to respond with a response that includes a shared secret. In some embodiments, the agent is required to respond with information regarding the presence, configuration, operating characteristics or other information regarding other programs in the operating environment of the agent. In some embodiments, the agent is required to respond with hashed information to be portions of code or a code sample (e.g., the code portion or code sample can be specified by the service controller 122).

[0177] In some embodiments, the information the agent responds with is a response to a signed or encrypted message from the service controller 122 in which the agent must know how to decode the encrypted controller message in order to respond correctly or it would be difficult for the agent to respond properly if the agent is not configured properly, is not operating within appropriate limits, is partially compromised or is entirely compromised. In some embodiments, the agent signs or encrypts information in such a manner that it is difficult to respond correctly when the message is decoded by the service controller 122 unless the agent is configured properly, is operating within appropriate limits, is not partially compromised and is not entirely

compromised. In some embodiments, the agent is required to respond with a signed or encrypted hash of information that is difficult for the agent to generate unless the agent is configured properly, is operating within appropriate limits, is not partially compromised and is not entirely compromised. For example, the hashed information can be local device configuration information, portions of code or all of the code, and/or the code portion to be used in the response can be specified by the service controller. In another example, the hashed information the agent responds with can include a shared secret, and/or the hashed information can be information regarding the presence, configuration, operating characteristics or other information regarding other programs in the operating environment of the agent.

[0178] Accordingly, as described above, the agent heartbeat function provides an important and efficient system in some embodiments for verifying the service policy implementation or protecting against compromise events. For example, there are many other functions the agent heartbeat service can perform and some are described herein while others will be apparent to one of ordinary skill in the art given the principles, design background and various embodiments provided herein.

[0179] In some embodiments, the service control device link 1691 facilitates another important function, which is the download of new service processor software elements, revisions of service processor software elements, and/or dynamic refreshes of service processor software elements. There are many embodiments for such operations. In some embodiments, the software is received as a single file over the service control device link 1691. For example, the file can have encryption or signed encryption beyond any provided by the communication link protocol itself. In some embodiments, the software files are segmented into smaller packets that are communicated in multiple messages sent over the service control device link 1691. In some embodiments, once the file(s) are received, or the segmented portions of the file(s) are received, they are communicated to a service downloader 1663 for file aggregation and installation, which, in some embodiments, is performed after further measures to verify the service processor software are completed. In some embodiments, the files are sent using other delivery means, such a direct TCP socket connection to the service downloader 1663 or some other software installer, which can also involve secure transport and additional levels of encryption.

[0180] As shown in FIG. 16, an agent communication bus 1630 represents a functional description for providing communication for the various service processor 115 agents and functions. In some embodiments, as represented in the functional diagram illustrated in FIG. 16, the architecture of the bus is generally multipoint to multipoint so that any agent can communicate with any other agent, the service controller or in some cases other components of the device, such user interface 1697 and/or modem components. As described below, the architecture can also be point to point for certain agents or communication transactions, or point to multipoint within the agent framework so that all agent communication can be concentrated, or secured, or controlled, or restricted, or logged or reported. In some embodiments, the agent communication bus is secured, signed, encrypted, hidden, partitioned and/or otherwise protected from unauthorized monitoring or usage.

[0181] In some embodiments, as described below, there are multiple layers of security applied to the agent communication bus 1630 communication protocols, such as including one or more of the following: point to point message exchange encryption using one or more keys that are partially shared or shared within the service processor 115 agent group and/or the service controller 122, point to point message exchange that using one or more keys that are private to the two endpoints of the communication, a bus-level message exchange encryption that can be in place of or in addition to other encryption or security, or using one or more keys that are partially shared or shared within the service processor 115 agent group and/or the service controller 122, a set of secure messages that can only be decoded or observed by the agents they are intended for, a set of secure messages that allow communication between certain agents or service processor functions and entities outside of the service processor operating environment. In some embodiments, and as described herein, the service control device link 1691 is assumed to be equivalent to an agent for communication purposes, and, in the case of the service control device link 1691, the communication is not restricted to the agent communication bus 1630 but also extends to the service control communications link 1653. In some embodiments, the system has the capability to replace keys or signatures on occasion or on a regular basis to further secure against monitoring, eavesdropping or compromise of the agent communication system.

[0182] For example, various forms of message encryption and security framework techniques can be applied to encrypt and/or secure the agent communication bus 1630, including

one or more of the following: agent bus encryption using shared key for all agents provided and updated by the secure server; agent bus encryption using point to point keys in which the secure server informs the bus and agents of keys and updates as appropriate; agent level encryption using agent to agent shared keys in which the secure server informs agents of the key and updates the key as appropriate; agent level encryption using agent to agent point to point key in which the secure server informs agent of the point to point keys that are required and updates the keys as appropriate; agent level access authorization, which only allows access to the agents that are on the secure authorization list and in which the list is provided by the secure server and signatures are provided by the secure server; UI messages are only analyzed and passed, in which the UI cannot have access to configuration information and cannot issue challenges; agent level heartbeat encryption, which can be point to point or shared key for that agent; control link level heartbeat encryption; TLS (Transport Layer Security) communication protocols; server level heartbeat encryption, which can be point to point or shared key for that secure server; and/or the access control integrity agent 1694 or heartbeat function can become point to multipoint secure communications hubs.

[0183] In some embodiments of the agent communication bus 1630, the design of the agent communication bus depends on the nature of the design embodiments for the agents and/or other functions. For example, if the agents are implemented largely or entirely in software, then the agent communication bus can be implemented as an inter-process software communication bus. In some embodiments, such an inter-process software communication bus is a variant of D-bus (e.g., a message bus system for inter-process software communication that, for example, helps applications/agents to talk to one another), or another inter-process communication protocol or system, running a session bus in which all communications over the session bus can be secured, signed, encrypted or otherwise protected. For example, the session bus can be further protected by storing all software (e.g., software components, applications and/or agents) in secure memory, storing all software in encrypted form in secure memory, and/or executing all software and communications within a secure execution environment, hardware environment and/or protected memory space. In some embodiments, if the agents and other functions are designed with a mixture of software and hardware, or primarily with hardware, then the implementation of the bus design will vary, and the principles and embodiments described herein

will enable one of ordinary skill in the art to design the specifics of the agent communication bus 1630 to meet a particular set of product and desired functional requirements.

[0184] As shown in FIG. 16, an access control integrity agent 1694 collects device information on service policy, service usage or service activity, agent configuration and agent behavior. In some embodiments, the access control integrity agent 1694 also cross checks this information to identify integrity breaches in the service policy implementation and control system. In some embodiments, the access control integrity agent 1694 also initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, the access control integrity agent 1694 also performs asynchronous or periodic agent checks to verify presence, configuration or proper operation of other agents. In some embodiments, the access control integrity agent 1694 also performs challenge-response sequence verification of other agents.

[0185] In some embodiments, the access control integrity agent 1694 obtains service usage or service activity measures from a service monitor agent 1696 and compares one or more first service usage measurement points against one or more second service usage measurement points to verify service policy implementation. For example, as shown in FIG. 21, if the service usage at measurement point IV is inconsistent with measurement point III, which, for example, can indicate, for example, that an unauthorized or unmonitored usage of the access modem (e.g., modems 2122, 2123, 2124, 2125 or 2141) is taking place. As another example, as also shown in FIG. 21, if one or more aspects of upstream traffic usage measurement point II, which represents the upstream demand side of policy implementation agent 1690, is inconsistent with upstream traffic measurement point III, which represents delivered traffic from the policy implementation agent 1690, then the policy implementation agent 1690 may not be operating properly. As another example, as also shown in FIG. 21, if service measurement point III and IV indicate that firewall agent 1655 is passing traffic to URLs or IP addresses that are in the blocked policy settings, then a verification error condition can be set for the access control policy. As another example, if the policy controller reports traffic usage statistics that are inconsistent with traffic usage policy settings, then a traffic usage policy verification error may have occurred. As another example, if the service usage counter synchronization information received from the service controller 122, the device service history 1618 and/or the central billing system 1619, is

compared to the service usage history reported by the service monitor agent and the two are found to be outside of acceptable tolerance limits for the comparison, then there may be a verification error in the service monitor service usage or service activity accounting. There are numerous additional embodiments of such comparisons as described herein and others as will be readily apparent to one of ordinary skill in the art given the principles, design background and specific examples and various embodiments described herein.

[0186] In some embodiments, device service policy implementations are verified by comparing various service usage measures used at the device against expected service usage or service activity behavior given the policies (e.g., one or more service policy settings, service profile or service profile settings for network based access/services, and/or service plan or service plan for network based access/services). For example, verification is performed based on a measure of total data passed at the device as compared to the service policy for total data usage. For example, verification is performed based on a measure of data passed in a period of time at the device as compared to the service policy for data passed in such a period of time. For example, verification is performed based on a monitoring of communications from the device based on IP addresses as compared to the policy for permissible IP addresses. For example, verification is performed based on a measure of total data passed from the device per IP address as compared to the policy for total data usage per IP address. Other examples include such actual versus policy comparisons based on other measures at/from/to the device, such as location, downloads, email accessed, URLs, and/or any other data, location, application, time or other criteria or any combination of criteria that can be measured for comparing with various policy settings and/or restrictions.

[0187] In some embodiments, the access control integrity agent 1694 monitors agent self-check reports to verify that agents are properly configured. In some embodiments, the access control integrity agent 1694 reports the agent self check reports to the service controller 122. In some embodiments, the access control integrity agent 1694 performs a role in service usage test transmission, reception and/or monitoring, with the usage test being tailored to test monitoring or control aspects for any subset of service activities. In some embodiments, the access control integrity agent 1694 performs a role in billing test event generation and/or monitoring. In some embodiments, the access control integrity agent 1694 checks and reports the result of service

usage monitoring verification tests, service usage billing verification tests and/or transaction billing verification tests.

[0188] In some embodiments, the access control integrity agent 1694 receives agent access attempt reports to determine if unauthorized agent access attempts are occurring. In some embodiments, the access control integrity agent 1694 acts as a central secure communications hub for agent to agent or service controller 122 to agent communication. For example, the access control integrity agent 1694 can be used so that no other software or function can access other agents or so that agents cannot access other agents except through the secure point to multipoint communications hub. In some embodiments, this approach further enhances compromise resistance for the agents. In some embodiments, some or all of the agent communications, including agent to agent or service controller 122 to agent communications, and possibly including unauthorized attempts to communication with agents, are monitored and logged so that a trace log of some or all agent communications can be maintained. For example, the agent communication trace log can be summarized and/or compressed for transmission efficiency or regularly reported, such as through the heartbeat function, or the agent communication trace log can be reported only when the service controller 122 requests the agent communication trace log or when there is a verification error event. As similarly described above, the partitioning of agent functions and server functions is provided herein mainly to aid in disclosing various embodiments but those of ordinary skill in the art will appreciate that other partitioning of agent functions and server functions can be used based on different design choices. For example, the central agent communication hub function is performed in some embodiments by the access control integrity agent 1694, however, in other embodiments that function is performed by the service control device link 1691. For example, when the central agent communication hub function is located in the service control device link 1691, then architecturally the device link can be a single point to multipoint secure communications hub for all agent to agent and service controller 122 to agent communications. In some embodiments, this approach has certain advantages from a service policy implementation verification or compromise protection robustness perspective, or has certain advantages from a communications protocol efficiency perspective, or simply can be more efficient to implement. It should be noted that in other embodiments described herein the agent to agent and agent to service controller 122 communications can be multipoint to multipoint, with each agent having the capability to

communicate with other agents or the service controller, this communication can be secure, signed or otherwise encrypted or protected in some embodiments and in the open/clear in others. Also, as discussed in some embodiments, the agents can maintain their own communications or attempted communications log, which can then be reported to the service controller 122. In some embodiments, the agents implement restrictions on which device components or agents the agents will conduct communications with so that only agents that need to communicate with one another can do so.

[0189] In some embodiments, the service control device link 1691 reviews local billing event history and compares such history to billing event reports to verify that a billing agent 1695 is functioning properly (e.g., has not been tampered with or compromised). In some embodiments, the service control device link 1691 cross-checks service usage or service activity against billing event reports from the billing agent 1695 to verify that billing events are properly billing for service usage or service activity. In some embodiments, the service control device link 1691 cross-checks transaction billing process or records against transaction billing reports to ensure that transaction billing events are being properly reported by the billing agent 1695. In some embodiments, the service control device link 1691 determines if one or more agents have been compromised, and if so, initiates a dynamic agent download process to replace any such potentially compromised agent.

[0190] In some embodiments, the access control integrity agent 1694 verifies that the service usage counter is reporting service usage or service cost to the user within acceptable limits of accuracy when compared to the service usage reports obtained from the service monitor agent 1696, the service controller 122, the device service history 1618 and/or the central billing system 1619. In some embodiments, the access control integrity agent 1694 checks to verify that user privacy filter preferences are being properly implemented. In some embodiments, the access control integrity agent 1694 checks to verify that the user is properly receiving UI warnings regarding service usage or roaming service usage conditions.

[0191] In some embodiments, the access control integrity agent 1694 checks to verify that the device is not beginning service usage until it has been authenticated, authorized or granted access to the network. In some embodiments, access control integrity agent 1694 checks

with the service controller 122 or the billing system 1619 to verify that the user or device has a valid service standing and should be admitted to access on the network.

[0192] In some embodiments, an Activation Tracking Service (ATS) is provided in which the service monitoring function (e.g., performed by the service monitor agent 1696 and/or some other agent/component or combinations thereof on the device) is used in part to determine which access networks are being connected to and to record and/or report this information. In some embodiments, the ATS is only enabled if the device user approves reporting of access networks connected to by the user device. In some embodiments, the ATS is protected from tampering. For example, the ATS can be hardened, that is, to be more tamper resistant, using a variety of techniques, including any of the following: the ATS can be located (e.g., stored) in secure memory and/or secure hardware; the ATS can be implemented in the system BIOS, the access modem and/or another hard to access portion of the device; a second device agent can confirm the presence of the ATS with a report to a network based server; the second agent or the network server can initiate a reinstall of the ATS if it is missing or is found to be operating improperly; and/or the ATS can be placed in a secure area of the OS so that it cannot be removed or if removed must be replaced for proper device operation to resume. A variety of other tamper resistance techniques can also be used to protect the ATS from tampering as similarly described herein with respect to other device based functions/software components/agents.

[0193] In some embodiments, the access control integrity agent 1694 verifies that ATS software or hardware is present, properly configured or operating properly. In some embodiments, the access control integrity agent 1694 reviews network connection or activity history and compares such to ATS reports to verify activation tracking service reports are occurring properly. In some embodiments, the access control integrity agent 1694 replaces ATS software if it has been removed. In some embodiments, the access control integrity agent 1694 monitors access or compromise of ATS software to determine if it may have been compromised. In some embodiments, the access control integrity agent 1694 reports status of ATS functions.

[0194] In some embodiments, the access control integrity agent 1694 scans the local agent execution environment to determine if there are unauthorized accesses to service processor functions, settings or code. In some embodiments, the access control integrity agent 1694

monitors software loading activity, protected memory access or communication with service processor 115 agents to detect unauthorized changes to service processor software or configuration. For example, the access control integrity agent 1694 can have a local database of potentially malicious elements and compare entries in the database against the elements detected locally. As another example, the access control integrity agent 1694 can communicate a list of some or all of the elements detected locally to the service controller 122 to augment or take the place of the database comparison function that may be performed locally. In some embodiments, the access control integrity agent 1694 detects new software downloads, installs or invocations and immediately issues an error flag report when potentially malicious software is downloaded, installed or invoked. In some embodiments, the access control integrity agent 1694 scans the local software loading and invocation activity along with a log of other software runtime events and regularly reports this trace so that when an error or compromise event occurs the trace preceding the event can be analyzed to determine the offending software or activity trace that took place to cause the compromise or error. Once the software or activity that caused the compromise is known, it can be entered into a refreshed version of the database that the device and other devices use to detect potentially malicious pre-cursor conditions. Examples of such pre-cursor events include software invocations, software downloads, attempts to uninstall certain agent and/or application software/components or OS components, a sequence of memory I/O events, a sequence of software access events, a sequence of network address or URL communications or downloads or a sequence of access modem I/O activity. In various other embodiments of the access control integrity agent 1694, the agent performs or (securely) communicates with other software/hardware device/network components that perform other well known signature, behavior blocking and/or intrusion detection identification/detection and/or blocking techniques based on the presence of potentially unwanted and/or potentially or known malicious software and/or intrusion attempts by unauthorized software and/or unauthorized users, using, for example, real-time, on access, periodic, and/or on demand scanning.

[0195] In some embodiments, the access control integrity agent 1694 detects or blocks potentially compromising behavior of other software programs/users attempting unauthorized behavior in the service processor 115 operating environment. In some embodiments, the access control integrity agent 1694 detects software that is being loaded that has the same or similar name, identification, memory location or function as one or more of the service processor 115

agents. In some embodiments, the access control integrity agent 1694 blocks operation or loading of such software. In some embodiments, the access control integrity agent 1694 detects or blocks unauthorized access of service processor 115 protected memory. In some embodiments, the access control integrity agent 1694 verifies configuration and operation of secure service downloader 1663. In some embodiments, the access control integrity agent 1694 monitors network and I/O activity to detect potentially compromising events, such as a program that is downloaded from known detrimental or potentially suspect IP addresses or URLs or a program that accesses certain IP addresses or URLs. In some embodiments, the access control integrity agent 1694 scans of the service processor operating environment are recorded and kept for a period of time, and if a service policy verification error occurs, then the scans immediately prior to the error are analyzed or reported to the service controller 122 for analysis. In some embodiments, such scans are regularly reported to the service controller 122 without the presence of service policy verification error conditions.

[0196] In some embodiments, the access control integrity agent 1694 requests a dynamic agent download of certain critical service processor functions, including in some cases the access control integrity agent 1694 on a periodic basis, or on a periodic basis when network access activity is not required or minimal.

[0197] In some embodiments, the access control integrity agent 1694 determines if a threshold has been surpassed for a max usage trigger for ambient and/or other services that should not be using significant amounts of data (e.g., based on the type of device and/or service profile settings).

[0198] In some embodiments, the access control integrity agent 1694 determines if verification errors exist in one or more of the verification process embodiments and, in some embodiments, reports errors immediately or in the next agent heartbeat to the service controller 122. In some embodiments, any number of results from the above checks, monitoring activities, reports or tests are reported to the service controller 122.

[0199] In some embodiments, a policy control agent 1692 receives policy instructions from the service controller 122 and/or the user via the billing agent 1695 and adapts device service policy settings (e.g., instantaneous device service policy settings) in one or more of the

following agents/components: a policy implementation agent 1690, the modem firewall 1655 and/or an application interface agent 1693. As shown in FIG. 16, the modem firewall 1655 is in communication with a modem driver 1640, which is in communication with the agent communication bus 1630 and access network 1610. As shown with respect to access network 1610, a central billing server 1619, an access network AAA server 1621 and device server history 1618 are also provided. As shown, the Internet 120 is accessible via the access network 1610 and firewall 124, from which device 100 can then access various Internet services 1615.

[0200] In some embodiments, the policy control agent 1692 adapts low level service policy rules/settings to perform one or more of the following objectives: achieve higher level service usage or cost objectives, reduce network control channel capacity drain, reduce network control plane server processing bandwidth, and/or provide a higher level of user privacy or network neutrality while satisfying service usage or service activity objectives. In some embodiments, the policy control agent 1692 performs a policy control function to adapt instantaneous service policies to achieve a service usage objective. In some embodiments, the policy control agent 1692 receives service usage information from the service monitor agent 1696 to evaluate service usage history as compared to service usage goals. In some embodiments, the policy control agent 1692 uses service monitor 1696 service usage or service activity history and various possible algorithm embodiments to create an estimate of the future projected service usage. In some embodiments, the policy control agent 1692 uses a future projection of service usage to determine what service usage or service activity controls need to be changed to maintain service usage goals. In some embodiments, the policy control agent 1692 uses service usage history to perform a service usage or service activity analysis to determine the distribution of service usage across service usage elements within categories, such as usage by application, usage by URL, usage by address, usage by content type, usage by time of day, usage by access network, usage by location, and/or any other categories for classifying service usage. In some embodiments, the policy control agent 1692 uses the service usage distribution analysis to determine which service usage elements or service activities are creating the largest service usage (e.g., if e-mail, social networking, or multimedia/online video application categories are creating the largest service usage).

[0201] In some embodiments, the policy control agent 1692 is instructed, for example, by the user, through billing agent 1695 to perform a service control algorithm, such as traffic shaping or download management, to manage service usage or service activities to assist the user in controlling service costs. As a basic example of such a traffic shaping algorithm, the traffic shaping algorithm can simply reduce traffic speed for all applications and traffic types successively until the service usage projections are within service usage limits for the present service billing period. To illustrate an algorithm that is more sophisticated and provides the advantage of leaving many service usage elements or service activities unaffected while only controlling down usage on the most aggressive service usage elements or service activities, the traffic shaping algorithm can identify the highest traffic usage applications and/or websites and successively reduce traffic speed just for the highest usage applications and/or websites until the service usage projections are within service usage limits for the present service billing period. These examples thereby reduce network traffic for the user in accordance with the user's service usage objectives while maintaining overall satisfactory service usage experience for the user in a manner that satisfies various net neutrality requirements (e.g., the traffic throttling of certain applications/websites based on user input in which categories based on service usage history are selected by the user, for example, a certain application may be using 90% of the aggregate traffic usage). For example, adaptive throttling algorithms can be used to throttle application traffic that the user requests throttling, such as recursively throttling of the specified application traffic (e.g., to denigrate the traffic usage associated with that application and thereby reduce overall service data usage).

[0202] In some embodiments, the policy control agent 1692 adjusts service policy based on time of day. In some embodiments, the policy control agent 1692 obtains a measure of network availability and adjusts traffic shaping policy settings based on available network capacity. In some embodiments, the policy control agent 1692 automatically and dynamically adjusts service policy based on one or more other service policy settings, the service profile and/or the service plan associated with the device and/or user of the device.

[0203] In some embodiments, various lower level service policy implementation embodiments are combined with a higher level set of service policy supervision functions to

provide device assisted verifiable network access control, authentication and authorization services.

[0204] In some embodiments, device based access control services are extended and combined with other policy design techniques to create a simplified device activation process and connected user experience referred to herein as ambient activation. In some embodiments, ambient access generally refers to an initial service access in which such service access is in some manner limited, such as where service options are significantly limited (e.g., low bandwidth network browsing and/or access to a specific transactional service), limited bandwidth, limited duration access before which a service plan must be purchased to maintain service or have service suspended/disabled or throttled or otherwise limited/reduced/downgraded, and/or any other time based, quality based, scope of service limited initial access for the network enabled device. In some embodiments, ambient activation is provided by setting access control to a fixed destination (e.g., providing access to a portal, such as a web page (e.g., for a hotspot) or WAP (Wireless Application Protocol) page, that provides the user with service plan options for obtaining a service plan for the user desired access, such as the service plan options for data usage, service types, time period for access (e.g., a day pass, a week pass or some other duration), and costs of service plan(s)). In some embodiments, service data usage of the ambient activated device is verified using IPDRs (e.g., using the device ID/device number for the device 100 to determine if the device has been used in a manner that is out of plan for the service plan associated with the device 100, such as based on the amount of data usage exceeding the service plan's service data usage limits, out of plan/unauthorized access to certain websites, and/or out of plan/unauthorized transactions). In some embodiments, service data usage of the ambient activated device is verified by setting a maximum data rate in the policy control agent 1692 and if/when it is determined that the device is exceeding a specified data rate/data usage, then the service data usage is throttled accordingly. In some embodiments, various other verification approaches are used for ambient activation purposes.

[0205] In some embodiments, the policy control agent 1692 (and/or another agent/component of the service processor 115 and/or service controller 122) performs a service control algorithm to assist in managing overall network capacity or application QoS (Quality of Service). In some embodiments, the policy control agent 1692 (and/or another agent/component

of the service processor 115) performs an access network selection algorithm to determine which access network to connect to based on connection options and determined strengths of available wireless networks, network preference or security settings, service usage cost based network preferences, and/or any other criteria.

[0206] Accordingly, as described herein with respect to various embodiments, service usage or service activities can be measured by various agents at various different measurement points, which provides for a more robust verification and integrity of device based services communication. For example, it is much less likely and more difficult to compromise and/or spoof multiple agents. As described herein, various verification and integrity checks are performed, including, for example, network based service usage measurement (e.g., using IPDRs); heartbeat monitoring; agent based heartbeat (e.g., challenge/response queries); agent operating environment protection; monitoring agent communications; agent cross-checks; comparing device based and network based measures (e.g., service usage measures); dynamic software/agent download; and/or any combination of these and various other verification/integrity check techniques described herein and/or apparent from the various embodiments described herein.

[0207] In some embodiments, the device 100 is capable of connecting to more than one network and device service policies are potentially changed based on which network the device is connected to at the time. In some embodiments, the network control plane servers detect a network connection change and initiate the service policy implementation established for the second network. In some embodiments, the device based adaptive policy control agent, as described herein (e.g., policy control agent 1692), detects network connection changes and implements the service policies established for the second network.

[0208] In some embodiments, when more than one access network is available, the network is chosen based on which network is most preferred according to a network preference list or according to which network that optimizes a network cost function. For example, the network preference list can be pre-established by the service provide and/or the user and/or later modified/adjusted by either the service provider and/or the user. For example, the cost function can be based on determining a minimum service cost, maximum network performance, whether

or not the user or device has access to the network, maximizing service provider connection benefit, reducing connections to alternative paid service providers, and/or any other cost related criteria for network selection purposes.

[0209] In some embodiments, the device 100 detects when one or more preferred networks are not available, implements a network selection function or intercepts other network selection functions, and offers a connection to the available service network that is highest on a preference list. For example, the preference list can be set by the service provider, the user and/or the service subscriber. In some embodiments, a notification is provided to the device/user when the device is not connected to a network (e.g., indicating in a pop-up/bubble or other UI based display a notification, such as “You are not connected to the network. Click here to learn more, get free trial, use a session, sign-up for service”). In some embodiments, the notification content can be determined based on usage service patterns, locally stored and/or programmable logic on the device and/or a server (e.g., device reports that user is not connected and WWAN is available). Decisions on what bubble to present when may be in pre-stored logic on device.

[0210] In some embodiments, service policies are automatically adapted based on the network to which device 100 is connected. For example, the device can be a cellular communication based device connected to a macrocell, a microcell, a picocell, or a femtocell (e.g., femto cells generally provide a low power, small area cellular network used, for example, in homes or offices, which, for example, can be used as an alternative to Wi-Fi access). In some embodiments, service monitoring agent 1696 and/or billing agent 1695 modify service usage counting and/or billing based on whether the device is connected to a macrocell, microcell, picocell or femtocell. In some embodiments, the device recognizes which type of network it is currently connecting to (e.g., looking up in a local or network table for the current base station connected to, and/or the information is broadcast to the device upon the connection with the base station), that is, whether it is a macrocell, microcell, picocell or femtocell. In other embodiments, the device does not recognize which type of network it is currently connected to, but reports its current base station, and the network uses a network lookup function to determine which type of network it is connected to. In some embodiments, the device adjusts the billing based on the type of network it is connected to, or in other embodiments, the device calculates an offset to such billing based on the type of network it is connected to, and/or in other

embodiments, the device records such service usage associated with the type of network it is connected to and the network billing can adjust the billing accordingly. For example, the billing can be lower for service data usage over a femtocell versus a macrocell. In some embodiments, service policies are adjusted based on the type of network that the device is connected, such as billing, user notification, data usage/bandwidth, throttling, time of day, who owns the cellular network connection (e.g., user's home femtocell, or user's work femtocell, or a commercial business's femtocell like a coffee shop or any other common area like an airport) and/or any other service policy can be different for a femtocell connection (or for any other type of connection, such as a macrocell, microcell, or picocell). In some embodiments, the local service usage counter is adjusted based on the type of network (and/or based on the time of day of such service activity) that the device is connected, such as billing, user notification, data usage/bandwidth, and/or any other service policy can be different for a femtocell connection (or for any other type of connection, such as a macrocell, microcell, or picocell). In some embodiments, the service policies and/or billing policies are adjusted based on network congestion.

[0211] In some embodiments, if adaptive service policy control is not required, then the policy control agent 1692 can simply pass instantaneous service policy settings directly to the agents responsible for implementing instantaneous service policies.

[0212] In some embodiments, a policy implementation agent 1690 implements traffic shaping and QoS policy rules for the device 100. In some embodiments, the policy implementation agent 1690 provides a firewall function. In some embodiments, the policy implementation agent 1690 performs traffic inspection and characterization. In some embodiments, packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed entirely in/by the policy implementation agent 1690. In some embodiments, the policy implementation agent 1690 accepts service policy implementation settings from the policy control agent 1692 or directly from the service controller 122. More detail on specific embodiments for the policy implementation agent 1690 is provided below with respect to the figures associated with communication stack and communication protocol flow.

[0213] In some embodiments, the burst size, buffer delay, acknowledgement delay and drop rate used in upstream and downstream traffic shaping are optimized with the goal of reducing access network traffic overhead, and excess capacity usage that can result from mismatches in traffic transmission parameters with the access network MAC and PHY or from excess network level packet delivery protocol re-transmissions. In some embodiments, the application interface agent 1693 is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. As shown in FIG. 16, the application interface agent 1693 is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[0214] In some embodiments, downstream literal or virtual application tagging are delayed until a traffic flow passes through the service policy implementation functions and to the application interface function where the service flow is then identified and associated with the underlying traffic and application parameters, and the literal or virtual tag is then communicated to the first policy implementation function or service monitoring function in the downstream traffic processing stack. In some embodiments, prior to being associated with a literal or virtual tag, the traffic flow is allowed to pass with no traffic shaping, and once the traffic flow is identified and tagged, the appropriate traffic shaping is applied. In some embodiments, a set of traffic shaping policy parameters are applied to the unidentified traffic flow before the flow is identified, and then the traffic shaping policy for the flow is updated when the flow is tagged. In some embodiments, the traffic flow can be blocked at the application interface agent even before the tag is passed to the policy implementation functions if it is found to be associated with traffic parameters that are blocked by policy once packet processing, framing and encryption are removed.

[0215] In some embodiments, a service monitor agent 1696 records and reports device service usage or service activities of device 100. In some embodiments, service usage history is verified by a number of techniques including verifying against network based service usage history (e.g., device service history 1618) and the various service policy implementation techniques as described herein.

[0216] In some embodiments, the service monitor agent 1696 includes the capability to filter service usage history reporting with the decision on which aspects of service history to report being determined by policies including possibly privacy policies defined by the device user or control plane servers in the network. In some embodiments, the service monitor agent 1696 monitors and possibly records or reports Customer Resource Management (CRM) information such as websites visited, time spent per website, interest indications based on website viewing, advertisements served to the device, advertisements opened by the user, location of the user, searches conducted by the user, application usage profile, device user interface usage history, electronic commerce transactions, music or video files played, applications on device, and/or when the user is actively working or playing or inactive. In some embodiments, to protect the privacy of this user CRM information, the user is provided with options on how much of the information to share and the user's response to the options are recorded and used to determine the filtering policy for how much of the CRM data to report (e.g., CRM filter level options selected by the user via the device UI and/or via various service plan or service profile or service policy options) and how much to suppress or to not even monitor/record/store in the first place. In some embodiments, to protect the privacy of this user's GPS/location tracking related information, the user is provided with options on how much of the information to share and the user's response to the options are recorded and used to determine the filtering policy for how much of the GPS/location tracking related data to report (e.g., GPS/location tracking filter level options) and how much to suppress or to not even monitor/record/store in the first place. In some embodiments, the service processor 115 allows the user to provide feedback on the user's preferences, such as for privacy/CRM data to report. In some embodiments, the user can also specify their preference(s) for notification (e.g., related to service usage/cost, traffic reporting and other service usage/monitored information) and/or service controls. In some embodiments, the service monitor agent 1696 observes and possibly records or reports service usage categorized by network possibly including roaming networks, paid service networks or free service networks. In some embodiments, the service monitor agent 1696 observes and possibly records or reports service usage categorized by sub-accounts for various types of traffic or various types of network.

[0217] For example, service monitor reports can be provided to the service controller 122. Service is monitored through various embodiments that can involve service usage logging

or traffic inspection and usage logging at the application level, various levels in the networking communication stack or the access modem. Some embodiments involve multiple levels of service or traffic measurement at various levels in the communications stack as described further below.

[0218] In some embodiments, service or traffic monitoring includes monitoring one or more of the following: traffic associated with one or more users; traffic downstream and/or upstream data rate; total traffic received and/or transmitted over a period of time; traffic transmitted and/or received by IP addresses, domain names, URLs or other network address identifiers; traffic transmitted and/or received by email downloads or uploads; traffic transmitted and/or received by an application; traffic transmitted and/or received by network file transfers; traffic transmitted and/or received by file download or upload content types; traffic transmitted and/or received by mobile commerce transactions; traffic transmitted and/or received by one or more time periods; traffic transmitted and/or received by differing levels of network activity and network capacity availability; traffic transmitted and/or received by one or more delivered levels of quality of service; traffic transmitted and/or received by software downloads; traffic transmitted and/or received by application downloads; traffic transmitted and/or received by one or more activities associated with the service control plane link or other network related functions, or traffic that may not directly result in service usage or service activity that the user values or desires; traffic transmitted and/or received to support one or more service provider third party service partner offerings; software usage history; application usage history; device discovery history for UI components, applications, settings, tutorials; ads served history; ads visited history; and/or device location history.

[0219] In some embodiments, some or all of the service usage monitoring occurs at the application layer. In some embodiments, the service monitor agent 1696 implements traffic inspection points between the applications and the networking stack application interface, such as the sockets API. In other embodiments, the application interface agent 1693 performs traffic inspection and reports the results to the service monitor agent 1696. Traffic inspection can be accomplished in several ways, including, for example, implementing a T-buffer at each socket connection and feeding the side traffic into a traffic flow analyzer, which in combination with a mapping of application to socket provides much of the information listed above. In cases in

which it is necessary to obtain traffic information from the application itself, some embodiments call for the application to be adapted to provide the information to either the application interface agent 1693 or the service monitor agent 1696. As an example, the application interface agent 1693 or the service monitor agent 1696 can monitor and decode advertisements downloaded via HTTP, but if the browser and HTTP server employ security above the sockets protocol stack layer then the application interface agent can communicate with the browser via a java applet or some other inter-process communication method. In some embodiments, the service monitor agent 1696, the billing agent 1695 and/or the policy control agent 1692 (or some other software or hardware function on the device) can monitor and/or control (e.g., allow, block and/or replace) advertisement traffic flow into the device. In some embodiments, the monitoring and control of advertisement traffic flow into the device is also used for bill by account purposes (e.g., charges, such as service charges, billed to the advertiser, sponsor, and/or service or transactional service provider).

[0220] In some embodiments, some or all of the service usage monitoring occurs below the application interface for the networking stack. In this case, some portion of the information listed above may not always be available due to encryption applied at the higher layers and/or the computational costs associated with performing deep packet inspection on mobile devices.

[0221] In some embodiments, the service monitor agent 1696 is also monitors the operating software install or loading systems, and/or otherwise monitors software installs or loads and/or software uninstalls/deinstallations.

[0222] Some of the information above may be considered by some users, advocacy groups or agencies as customer sensitive personal information. Simply sending the above information to the network for unspecified purposes may not, therefore, be acceptable for some service providers. However, if the user provides specific approval (e.g., informed consent) for the device, network or service provider to use some or all of the information that may be sensitive for specified purposes, then the user can control the level of information that is used and the purpose the information is used for. Accordingly, various embodiments described herein provide the user with control of what information is used and the purposes it is used for thereby allowing the user adequate control of any such sensitive information. In some embodiments,

information that is thought to perhaps be sensitive and is reported to the network must first receive user approval for the reporting. Some basic information is generally not considered sensitive and is necessary for certain basic service provider needs. For example, total data transmitted and/or received, traffic downstream and/or upstream speed, overall traffic usage by time of day are generally not considered private from the service provider's perspective and are necessary in many basic service policy implementations. As additional examples, perhaps other service usage history, such as total traffic email downloads and uploads but not the type of files or any specifics about the email traffic, the total web browsing traffic but nothing specific about the sites visited or content viewed, total file transfer traffic but not the type of files transferred or the addresses involved in the transfer, and other examples may not be viewed as private and, in some embodiments, provide valuable information for the service provider to manage services. Conversely, information such as websites visited, content viewed, mobile commerce transactions completed, advertisements visited, GPS location history and other service usage history the service monitor is capable of recording may be sensitive or private for some users and would thereby benefit from the various embodiments that provide enhanced user control of the reporting of such potentially sensitive or private data. It should also be appreciated that there is an inherent advantage to implementing traffic monitoring, traffic, service monitoring or service control on a device, because it is not necessary to report sensitive information to the network to accomplish many of these service policy implementation objectives.

[0223] In some embodiments, the service monitor agent 1696 assists in virtual application tagging of traffic flows through the networking stack policy implementation by tracking the virtually tagged packets through the stack processing and communicating the flow tags to the service policy implementation agent(s) 1690. In some embodiments, the service monitor agent 1696 maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the service controller 122 to which the device has connected. In some embodiments, this network activity summary includes a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. In some embodiments, the traffic reports that go to the network, possibly to service controller 122, billing system 1619 and/or device service history 1618, are first filtered according to rules defined by user preference selection at the time of service activation (e.g., service plan/service plan option selection), time of first device use, at a time the user selected the option on the

service UI or at a time the user chose to change the option on the service UI or some other time/mechanism allowing for user preference selection.

[0224] In some embodiments, the service monitor agent 1696 monitors application usage (e.g., which application the user executes on the device 100, such as e-mail applications, web browsing applications and/or media content streaming applications). In some embodiments, the service monitor agent 1696 monitors multimedia file usage (e.g., based on multimedia file type and/or based on specific multimedia files, such as specific movies and/or songs). In some embodiments, the service monitor agent 1696 monitors the device user interface, application, and content discovery history (e.g., monitoring which applications/content the user accesses from the device, including monitoring the pattern by which the user accesses such applications/content, such as how the user navigates the user interface on the device to access such applications/content and maintaining such patterns and history, such as which icons the user access on a home page, secondary or other portion/mechanism on the device for accessing various applications/content). In some embodiments, the service monitor agent 1696 monitors advertisements provided to the user on the device 100. In some embodiments, the service monitor agent 1696 monitors advertisements viewed (e.g., accessed, such as by clicking on a web advertisement) by the user on the device 100. In some embodiments, the service monitor agent 1696 monitors GPS/location information for the device 100. As will be appreciated by those of ordinary skill in the art, the service monitor agent 1696 can monitor a wide variety of activities performed by the device/user of the device and/or based on other information related to the device 100 such as GPS/location information. As described herein, in some embodiments, the user of the device 100 can also specify which activities that the user authorizes for such monitoring (e.g., the user may prefer to not allow for such GPS/location monitoring).

[0225] In some embodiments, the application interface agent 1693 provides an interface for device application programs. In some embodiments, the application interface agent 1693 identifies application level traffic, reports virtual service identification tags or appends literal service identification tags to assist service policy implementation, such as access control, traffic shaping QoS control, service type dependent billing or other service control or implementation functions. In some embodiments, the application interface agent 1693 assists with application layer service usage monitoring by, for example, passively inspecting and logging traffic or

service characteristics at a point in the software stack between the applications and the standard networking stack application interface, such as the sockets API. In some embodiments, the application interface agent 1693 intercepts traffic between the applications and the standard network stack interface API in order to more deeply inspect the traffic, modify the traffic or shape the traffic (e.g., thereby not requiring any modification of the device networking/communication stack of the device OS). In some embodiments, the application interface agent 1693 implements certain aspects of service policies, such as application level access control, application associated billing, application layer service monitoring or reporting, application layer based traffic shaping, service type dependent billing, or other service control or implementation functions.

[0226] In some embodiments, application layer based traffic monitoring and shaping can be performed as described below. The traffic from each application can be divided into one or more traffic flows that each flow through a traffic queue, with each queue being associated with one or more additional classifications for that application (e.g., the application can be a browser that is associated with multiple queues representing different destinations or groups of destinations it is connected to, with each destination or group of destinations having potentially different access control or traffic control policies, or the application can be associated with different content types or groups of content types with each content type having different queues, the application might be an email program with email text traffic going to one queue and downloads going to another with different policies for each). In some embodiments, queues are formed for all applications or groups of applications that are associated with one or more traffic parameters such as destination, content type, time of day or groups of applications can be similarly assigned to different queues. The functions performed by the application layer queues can be similar to the functions described for the policy implementation agent, such as pass, block, buffer, delay, burst in order to control the traffic or network access associated with the queue. The drop function can also be implemented, such as for application layer protocols that include reliable transmission methods, but if the application layer protocol does not involve reliable retransmission of lost information this can result in lost data or unreliable communication which may be acceptable in some cases. The manner in which the queues are controlled can be constructed to result in a similar approach for controlling services or implementing service activity control similar to the other embodiments described herein,

including, for example, the policy control agent 1692 implementing an higher layer of service control to achieve a higher level objective as discussed herein.

[0227] In some embodiments, the application interface agent 1693 interacts with application programs to arrange application settings to aid in implementing application level service policy implementation or billing, such as email file transfer options, peer to peer networking file transfer options, media content resolution or compression settings and/or inserting or modifying browser headers. In some embodiments, the application interface agent 1693 intercepts certain application traffic to modify traffic application layer parameters, such as email file transfer options or browser headers. In some embodiments, the application interface agent 1693 transmits or receives a service usage test element to aid in verifying service policy implementation, service monitoring or service billing. In some embodiments, the application interface agent 1693 performs a transaction billing intercept function to aid the billing agent 1695 in transaction billing. In some embodiments, the application interface agent 1693 transmits or receives a billing test element to aid in verifying transaction billing or service billing.

[0228] In some embodiments, a modem firewall 1655 blocks or passes traffic based on service policies and traffic attributes. In some embodiments, the modem firewall 1655 assists in virtual or literal upstream traffic flow tagging. Although not shown in FIG. 16, in some embodiments, the modem firewall 1655 is located on either side of the modem bus and in some embodiments it is advantageous to locate it on the modem itself.

[0229] In some embodiments, the billing agent 1695 detects and reports service billing events. In some embodiments, the billing agent 1695 plays a key role in transaction billing. In some embodiments, the billing agent 1695 performs one or more of the following functions: provides the user with service plan options, accepts service plan selections, provides options on service usage notification policies, accepts user preference specifications on service usage notification policies, provides notification on service usage levels, provides alerts when service usage threatens to go over plan limits or to generate excess cost, provides options on service usage control policy, accepts choices on service usage control policy, informs policy control agent 1692 of user preference on service usage control policy, provides billing transaction options and/or accepts billing transaction choices. In some embodiments, the billing agent 1695

interacts with transaction servers (e.g., open content transaction partner sites 134) to conduct ecommerce transactions with central billing 1619.

[0230] In some embodiments, service processor 115 includes one or more service usage or service activity counters. For example, the service monitor agent 1696, billing agent 1695 or a combination of these agents and/or other agents/components of service processor 115 can include such a local service usage counter(s) for the device 100. In some embodiments, a service usage counter monitors service usage including data usage to/from the device 100 with the access network 1610. In some embodiments, the service usage counter periodically, in response to a user request, in response to a service processor 115 agent's request (e.g., the billing agent 1695, the policy control agent 1692, or another agent of service processor 115), in response to the service controller 122, and/or in response to the central billing 1619 (e.g., for billing purposes and/or for storing in the device service history 1618), provides a service usage report, including monitored service usage for the device 100. In some embodiments, the service usage counter periodically, or in response to a request, synchronizes the service usage counter on the device 100 with a network (and/or billing) service usage counter, such as that maintained potentially at central billing 1619. In some embodiments, service processor 115 utilizes the service usage counter to provide a service usage projection. In some embodiments, service processor 115 utilizes the service usage counter to provide a service usage cost estimate. In some embodiments, service usage projections from policy control agent 1692 are used to estimate the projected future service usage if user service usage behavior remains consistent. In some embodiments, service processor 115 utilizes the service usage counter to provide a cost of service usage, and the service processor 115 then periodically, or in response to a request, synchronizes the cost of service usage with, for example, the central billing 1619. In some embodiments, the service processor 115 utilizes the service usage counter to determine whether the user is exceeding and/or is projected to exceed their current service plan for data usage, and then various actions can be performed as similarly described herein to allow the user to modify their service plan and/or modify (e.g., throttle) their network data usage. In some embodiments, the service usage counter can support providing to the user the following service usage related data/reports: service usage, known usage and estimated usage, projected usage, present costs, projected costs, cost to roam, cost to roam options, and/or projected roaming costs. For example, including a local service data usage counter on the device 100 allows the service processor 115

to more accurately monitor service data usage, because, for example, network (and/or billing) service usage counters may not accurately also include, for example, control plane data traffic sent to/from the device 100 in their monitored service data usage count.

[0231] In some embodiments, verifiable device based service billing solutions are provided. For example, as described herein, various device based service billing solutions can include a wide range of verification techniques to ensure that the device is properly reporting service billing events (e.g., to verify/ensure that the service billing is not malfunctioning and/or has not been tampered with/compromised such that it is not accurately or timely providing service billing information). As described herein, service billing generally refers the billing for one or more services for a device, such as device 100 (e.g., email service billing for data usage associated with received/sent email related data over the access network 1610, web browsing service billing for data usage associated with received/sent web browsing related data over the access network 1610 and/or any other network based service, and/or any transactional based services, such as for multimedia content purchases or other transactions).

[0232] In some embodiments, verifiable device based service billing is provided by sending dummy(/test) billing events, such as having an access control integrity server 1654 of the service controller 122 instruct the access control integrity agent 1694 to send a dummy(/test) billing event to the billing agent 1695. If the billing agent does not then send the expected report, which should reflect the dummy(/test) (or fails to timely send any report), then the system can verify whether the billing process is working properly. In addition, a dummy (/test) transaction can be used to verify transaction based billing through a variety of approaches (e.g., the access control integrity agent 1694 can similarly send a dummy(/test) transactional billing event to the billing agent 1695 as a test to determine whether the billing agent 1695 then provides the expected report reflecting that dummy(/test) transaction). For example, the test billing events can be trapped by a device assisted billing mediation server and removed from the user account billing.

[0233] In some embodiments, verifiable device based service billing is provided by sending one or more data bursts to the device to confirm that data was received and to confirm that the service monitor agent 1696 properly logged the data burst(s) in the local service usage or

service activity counter. In some embodiments, data bursts can be used to verify data throttling (e.g., if the device has exceeded service data usage limits and/or is approaching such limits such that service data usage should be throttled, then sending data bursts can be used to verify whether the expected throttling is properly being performed on the device). In some embodiments, verifiable device based service billing is provided by submitting requests to connect to an unauthorized service/website to verify if that unauthorized service usage is properly blocked. In some embodiments, verifiable device based service billing is provided by submitting requests to perform an unauthorized transaction to verify if that unauthorized transaction is properly blocked.

[0234] In some embodiments, verifiable device based service billing is provided by verifying device service activities relative to IPDRs for the device. In some embodiments, the IPDRs for the device (possibly in a modified format) are periodically and/or upon request sent to the device, as described herein. For example, IPDRs for the device can be compared to the device's local service data usage counter and/or to the service plan for the device to determine if the overall service data usage limit has been exceeded, whether out of plan/unauthorized/unrecorded websites/other services have been performed by the device, whether service plan/profile bandwidth limits have been exceeded, whether out of plan/unauthorized/unrecorded transactions have been performed (e.g., verifying IPDR transaction logs, assuming such are included in the IPDRs, with the local transaction logs of the device to determine, for example, whether the local device records indicate that fewer than the network recorded number of content downloads, such as downloaded songs, were purchased), and/or whether any other activities verifiable based on a comparison of IPDRs indicate that the device has been used in any manner that is out of or exceeds the service plan/profile for the device.

[0235] In some embodiments, device based service billing includes recording billing option response history. For example, this approach can be particularly important for service plan overage conditions (e.g., when the use of the device is exceeding the service plan associated with the device in some manner, such as service data usage, bandwidth, service or transaction access and/or in some other manner). In some embodiments, in a service plan overage condition, the user is requested to confirm that user has acknowledged notification of service plan overage,

such as via the user interface 1697. In some embodiments, such service plan overage acknowledgements require that the user enter a unique identification to validate authorization by the user identity associated with the device (e.g., another type of verification mechanism, in the event a device is stolen or being used by someone other than the authorized user of the device, then that unauthorized user would not be able to confirm the service plan overage acknowledgement, and appropriate actions can then be taken, such as throttling, quarantining or (temporarily) suspending service/network access). In some embodiments, if the device is compromised/hacked (e.g., by the user of the device), and the device is used in a manner that results in a service usage overage (e.g., determined based on device assisted service usage monitoring, and/or network based service usage monitoring using IPDRs/CDRs), then the billing system determines billing for such service usage overage costs. This overage billing can be initiated by the device 100 (e.g., service processor 115), the service controller 122, the billing system 123, the AAA 121, or some other network function. In some embodiments, if the device is compromised/hacked (e.g., by a user of the device), and the device is used in a manner that results in a service usage overage, one or more of the following actions is taken: the user is notified, the user is required to acknowledge the notification, the device traffic is sent to SPAN (or similar traffic sampling and analysis function), and/or the device is flagged for further analysis.

[0236] In some embodiments, device based service billing includes an option to bill by account, such as to bill different service activities and/or transactions to a specified account (e.g., other than the user's account associated with the general service plan for the device). For example, bill by account can provide for billing according to application, content type, website, transaction, network chatter (e.g., heartbeat communications and/or other network traffic that is used by, for example, the central/service provider to generally maintain network access for the device), and/or transaction partner sponsored activities and then report such bill by account information for billing mediation/reconciliation. For example, a bill by account report can be sent by billing agent 1695 from the device to central billing 1619 (e.g., as a billing event); or alternatively, sent to an intermediate server/aggregator, which can then reformat and send the reformatted report to central billing 1619 (e.g., providing the billing report in a format required by central billing 1619); or alternatively, sent to a mediation server, which can re-compute the billing based on the bill by account report (e.g., offset the bill based on network chatter,

transaction based billing, transaction partner sponsored activities, content providers, website providers and/or advertising providers) and then send the recomputed (and potentially reformatted) report to central billing 1619.

[0237] In some embodiments, one or more of the mediation/reconciliation functions for device assisted billing, device generated billing events, device generated bill by account events and device generated open transaction billing events can be implemented in the service controller 122 (e.g., the billing event server 1662) or in another function located in the billing system 123 or elsewhere. This billing mediation server function accepts the device based billing events discussed immediately above, reformats the billing events into a format accepted and recognized by the billing system, mediates the billing event information to remove service usage billing from the user account and place it in other bill by account categories as appropriate according to the bill by account mediation rules, adds other billing events for service usage or transactions to the user account as appropriate according to the device based billing rules, and then applies the information to the billing information the user account to correct or update the account.

[0238] For example, a bill by account can allow for a website provider, such as Google or Yahoo, to pay for or offset certain account usage for web browsing, web based searching, web based email, or any other web based or other service usage activities, which may also be based (in whole or in part) on the activities performed by the user on such transactional services (e.g., based on advertisement viewing/accessing or click-through activities by the user, by which an advertisement business model used by such website providers directly or indirectly supports such service account subsidies). As another example, a bill by account can allow for an advertiser to pay for or offset certain account usage for viewing and/or accessing (e.g., clicking through) a web placed advertisement or other advertisement sent via the network to the device. As yet another example, various network chatter (e.g., heartbeat related network and other network chatter related service data usage) can be assigned to a dummy account and such can be used to offset the bill and/or used for tracking the data usage for such activities for the device. In another example, service data usage for access to a transactional service, such as a multimedia content download service (e.g., music, eBook, music/video streaming, and/or movie or other multimedia content download service), or an online shopping site (e.g., Amazon, eBay or another online shopping site), can be billed to a transactional service account assigned to a transactional

service partner that sponsors access to that sponsor's transactional service, thereby allowing that transactional service partner to pay for or offset (e.g., subsidize) the account usage for such activities, which may also be based (in whole or in part) on the transactions actually performed by the user on such transactional services (e.g., based on the volume/cost of the multimedia service download purchases by the user and/or online activities).

[0239] In some embodiments, device based service billing includes recording billing events on the device and then reporting such billing to the network (e.g., central billing 1619). In some embodiments, device based service billing includes reporting service usage events and/or applying cost look-up and logging/reporting service billing updates. For example, this allows for reporting not only service usage but also cost of such service usage to the user via the user interface of device 100. Also, for example, the cost of such service usage can also be reported to the billing server. In some embodiments, device based service billing includes reporting service usage to the network, and the network determines the cost for such service usage.

[0240] In some embodiments, billing information for roaming partners is provided. For example, a roaming server can include a roaming service cost data table for roaming service partners. In this example, when the device (e.g., device 100) connects to a roaming network provided by a roaming service partner, then the device can also receive the roaming service data rate based on the roaming service cost data table provided by the roaming server. Alternatively, the roaming server can send the roaming service cost data table (or a modified format of the same) to the device thereby allowing the device to determine the costs for such roaming network service usage or service activity. As described herein, the device can also automatically use a roaming service profile when connecting to the roaming network service and/or the user can be notified of the roaming service profile options based on the roaming service data costs and then select the desired roaming service profile accordingly.

[0241] In some embodiments, the user is provided with a list of service costs based on locally stored roaming table and a search of available roaming partners that the device 100 detects and can connect to. In some embodiments, the user is provided with a projected cost per day for one or more roaming service provider options based on typical service usage history and the cost for each service provider. In some embodiments, the user is provided with a set of

options for service usage notification, controlling or throttling service usage and/or cost while roaming (e.g., using the service notification and cost control techniques as similarly discussed herein but applied to the roaming network). In some embodiments, these controls are set by a VSP (or, e.g., an IT manager using VSP functions). In some embodiments, roaming tables are updated periodically in the background while on a home network (or other low cost network) and cached. In some embodiments, cache updates occur based on fixed time period (e.g., late at night when updates are less expensive due to network inactivity). In some embodiments, the roaming partner cost table cache updates are done whenever connected to a desirable network that is not as expensive or bandwidth constrained (e.g., at home, work, or off the WWAN). In some embodiments, updates occur at time of day that network is not busy. In some embodiments, updates occur based on network push when roaming table is changed (e.g., one or more of the roaming partners changes the rate). In some embodiments, the service cost to update the roaming service cost table is charged to bill by account and possibly not charged to end user. In some embodiments, the roaming service center is provided as a service that is paid for (e.g., potentially bill by account tracks all related costs). For example, this type of roaming cost control can be provided as a service through central provider, MVNO, roaming partner provider, VSP or as a third party application not associated with any service provider (e.g., IT manager). For example, the controls for how to update cache, set service control policies, and other controls can be defined by any number of VSP entities including the user through a website service.

[0242] In some embodiments, a roaming service center is provided as a service in which, for example, the user is provided with a list of service costs based on a locally stored (or remotely accessed) roaming table. In some embodiments, the roaming service center provides the user with a projected cost per day for one or more roaming service provider options based on typical service usage history and the cost for each service provider. In some embodiments, the roaming service center provides the user with a set of options for controlling/throttling usage and/or cost while roaming. In some embodiments, these controls are set by a VSP (e.g., an IT manager using VSP functions). For example, roaming tables can be updated periodically in the background while on a home network and cached. In some embodiments, cache updates occur based on a fixed time period. In some embodiments, the roaming partner cost table cache updates are done whenever the device is connected to a desirable network that is not as

expensive or bandwidth constrained (e.g., at home, work and/or off the WWAN). In some embodiments, updates occur at time of day that network is not busy. In some embodiments, updates occur based on a network push when a roaming table is changed (e.g., one or more of the roaming partners changes the rate). In some embodiments, the service cost to update the roaming service cost table is charged to bill by account and possibly not charged to the user. In some embodiments, the roaming service center is provided as a service that is paid for by the user and/or part of a service plan. In some embodiments, a bill by account function tracks all related costs. For example, the roaming service center can be provided as a service through central provider, MVNO, roaming partner provider, VSP or as a third party application not associated with any service provider (e.g., IT manager).

[0243] In some embodiments, a synchronized local service usage counter based on time stamped central billing information is provided. For example, the local service usage counter, as similarly described above, can also be synchronized to past service usage records (e.g., time stamped central billing records of service usage for the device) and use local estimates for current/present service usage estimates for the device. In this example, the central billing system (e.g., central billing 1619) can push the time stamped central billing information to the device (e.g., device 100), the device can pull the time stamped central billing information, and/or an intermediate server can provide a mediated push or pull process. In some embodiments, synchronization is performing periodically based on service usage levels with free-running estimates between synchronizations.

[0244] In some embodiments, service usage is projected based on calculated estimates of service usage based on synchronized service usage and local service usage count information. For example, projected service usage can be calculated on the device or calculated on a server (e.g., a billing server or an intermediate billing server), which provides the calculated projected service usage information to the device, such as using various adaptive algorithms for service usage projections. For example, an adaptive algorithm can use historical/past synchronized network service usage information (e.g., synchronized with local service usage data based on time stamps associated with IPDRs) to assist in service usage projections, based on, for example, total service usage count, service usage count by certain service related criteria (e.g., application, content, service type, website and/or time of day). In another example, an adaptive algorithm

synchronizes to past service usage data (e.g., the local estimate of past service usage data is updated to be synchronized up through the point in time associated with the latest IPDR time stamp that has been received) and current local estimates of service usage collected since the latest time stamp are then added to the time stamped IPDR service usage counter to minimize the service usage counter offset so that it is no greater than the difference between the network service usage measure and the local service usage measure since the latest IPDR time stamp. In some embodiments, these adaptive algorithm techniques are performed on the device and/or performed on the network (e.g., on a network server) for processing. In some embodiments, if there is an offset in the local device based service usage count between IPDR synchronization events and the IPDR service usage count between IPDR synchronization events, then an algorithm can be employed to estimate any systematic sources for the offset and correct the local service usage count to minimize the offsets. As an example, if the IPDR service usage count is typically off by a fixed percentage, either high or low, then an algorithm can be employed to estimate a multiplier that is applied to the local service usage count to minimize the offset between IPDR service usage synchronization events. In another example, there can be a consistent constant offset and a multiplier offset, both of which can be estimated and corrected for. Those of ordinary skill in the art will appreciate that more sophisticated algorithms can be employed to estimate the nature of any systematic offsets, including, for example, offsets that occur due to specific service usage activities or network chatter to manage the device, and such offsets can then be minimized between IPDR service synchronization events. In some embodiments, synchronized service usage data is used to create an improved analysis of the statistical patterns of service usage to provide more accurate service usage projections. Those of ordinary skill in the art will also appreciate that a variety of additional adaptive algorithm techniques can be used including those that provide for various statistical analysis techniques and/or other techniques.

[0245] In some embodiments, service usage is projected for the end of a billing/service period for a service plan versus the service usage allowed under the service plan for that billing/service period. A display of excess charges is also provided for the projected rate of service usage based on the monitored service usage behavior through the end of the billing/service period (e.g., this can be zero if the service usage is projected to be less than that allowed under the service plan and a positive cost number if it is projected to be more than the

service plan). For example, this can be implemented in numerous ways, such as on a server in the network, on a gateway/router/switch in the network, and/or on the device, as discussed below and generally described herein with respect to other service/cost usage monitoring and notification embodiments. If implemented in the network server or gateway/router/switch, then the service/cost usage projections and related information can be pushed to the device, or the device can be notified that such information is available to pull and/or periodically pushed/pulled. The service usage information/estimates can be collected from the device, the network or both (e.g., reconciled and/or synchronized) as similarly described herein. The service usage information/estimates are then analyzed to determine service usage/cost projects as similarly described herein and compared to the service plan for the device to determine the projected service/cost usage overage (if any). In some embodiments, one or more of the following are determined by, reported to and/or displayed on the device: service usage value, projected service usage value, service usage plan limit, projected service usage overage, projected service cost overage, service plan period time duration, service plan time remaining before end of period and/or other pertinent information.

[0246] In some embodiments, the device also determines service costs based on the synchronized service usage count thereby allowing the device to also report the service cost information to the user. For example, the device can locally store a service cost look-up table(s), locally store different service cost look-up tables for different networks and/or for roaming networks, and/or request such information from a billing or intermediate billing server (and/or a roaming server) on the network. As another example, the device can obtain the calculated service costs based on the synchronized local service usage count and/or network service usage count from an intermediate server (e.g., a billing or intermediate billing server) thereby offloading the computational costs associated with calculated these projections and the data storage for service cost lookup tables onto the intermediate server on the network using the network service usage counter with or, alternatively, without the synchronized local service usage counter.

[0247] In some embodiments, service usage count categorization by network (e.g., a home network (such as a Wi-Fi, WAN, femtocell or other home network) versus a roaming network) is provided. Similarly, the synchronized local service usage counter can be

synchronized by network. Also, a synchronized local service usage count for networks controlled by a central provider, for networks controlled by other providers (e.g., MVNO), and/or free networks can similarly be provided.

[0248] In some embodiments, a service notification and billing interface is provided. For example, service usage and projected service usage, such as described herein, can be displayed to the user of the device (e.g., via user interface 1697). Similarly, expected/projected service or cost overrun/overage, such as described herein, can also be displayed to the user. As another example, a most cost effective plan can be determined/projected based on historical and/or projected service usage, and this determined/projected most cost effective plan can be displayed to the user. In yet another example, a list of available networks accessible by the device can be displayed to the user. In this example, one or more undesired available networks can also be blocked from display thereby only displaying to the user desired and/or preferred available networks. In this example, service usage plans and/or service usage plan option comparison for one or more alternative networks or roaming networks can also be displayed to the user. Similarly, service cost plans and/or service/cost plan option comparison for one or more alternative networks or roaming networks can also be displayed to the user. In addition, roaming service usage, projected roaming service usage, estimated roaming service cost, and/or projected estimated roaming service cost can also be displayed to the user. These roaming service usage/costs can also be displayed to the user so that the user can utilize this information for selecting various roaming service billing options. In another example, alternative and/or least cost networks are determined and displayed to the user. In another example, alternative warnings are displayed to the user for any or specified roaming networks.

[0249] In some embodiments, the service notification and billing interface notifies the user of expected network coverage (e.g., based on the device's current geography/location and the accessible networks for the device from that current geography/location) and displays options to the user based on the expected network coverage information. In some embodiments, the service notification and billing interface notifies the user of their current service usage at specified service usage points and displays various options to the user (e.g., service usage options and/or billing options). For example, the user's responses to the presented options are recorded (e.g., stored locally on the device at least temporarily for reporting purposes or

permanently in a local configuration data store until such configuration settings are otherwise modified or reset) and reported, such as to the billing server (e.g., central billing 1619). For example, user input, such as selected options and/or corresponding policy settings, can be stored locally on the device via a cache system. As another example, the service notification and billing interface displays options to the user for how the user wants to be notified and how the user wants to control service usage costs, the user's input on such notification options is recorded, and the cost control options (e.g., and the billing agent 1695 and policy control agent 1692) are configured accordingly. Similarly, the user's input on service plan options/changes can be recorded, and the service plan options/changes (e.g., and the billing agent 1695 and policy control agent 1692) are configured/updated accordingly. In another example, the service notification and billing interface provides various traffic control profiles, such as for where the user requests assistance in controlling service usage costs (e.g., service data usage and/or transactional usage related activities/costs). Similarly, the service notification and billing interface can provide various notification options, such as for where the user wants advance warning on service coverage. In another example, the service notification and billing interface provides options for automatic pre-buy at a set point in service usage. In another example, the service notification and billing interface provides the option to choose different notification and cost control options for alternative networks or roaming networks.

[0250] In some embodiments, an online portal or web server is provided for allowing the user to select and/or update policy settings. For example, user input provided via the online portal/web server can be recorded and reported to the billing server (e.g., central billing 1619). In another example, the online portal/web server can display transaction billing information and/or accept input for a transaction billing request, which can then be reported to the billing server accordingly.

[0251] As shown in FIG. 16, the service processor 115 includes a service interface or user interface 1697. In some embodiments, the user interface 1697 provides the user with information and accepts user choices or preferences on one or more of the following: user service information, user billing information, service activation, service plan selection or change, service usage or service activity counters, remaining service status, service usage projections, service usage overage possibility warnings, service cost status, service cost projections, service

usage control policy options, privacy/CRM/GPS related options, and/or other service related information, settings, and/or options. For example, the user interface 1697 can collect service usage information from service monitor agent 1696 to update the local service usage counter (and/or, alternatively, the service usage information is obtained from the service controller 122) to update user interface service usage or service cost information for display to the user. As another example, service billing records obtained from central billing system 1619 can be used to synchronize local service usage counters and service monitor agent 1696 information to perform real-time updating of local service usage counters between billing system 1619 synchronizations. As another example, the user interface 1697 can display options and accept user preference feedback, such as similarly discussed above with respect to user privacy/CRM/GPS filtering, traffic monitoring and service controls. For example, the user interface 1697 can allow the user of the device to modify their privacy settings, provide user feedback on service preferences and/or service experiences, modify their service profiles (e.g., preferences, settings, configurations, and/or network settings and options), to review service usage data (e.g., based on local service usage counters and/or other data monitored by the service processor 115), to receive various events or triggers (e.g., based on projected service usage/costs), and/or the user interface 1697 can provide/support various other user input/output for service control and service usage.

[0252] In some embodiments, by providing the service policy implementation and the control of service policy implementation to the preferences of the user, and/or by providing the user with the option of specifying or influencing how the various service notification and control policies or control algorithms are implemented, the user is provided with options for how to control the service experience, the service cost, the capabilities of the service, the manner in which the user is notified regarding service usage or service cost, the level of sensitive user information that is shared with the network or service provider entity, and the manner in which certain service usage activities may or may not be throttled, accelerated, blocked, enabled and/or otherwise controlled. Accordingly, some embodiments provide the service control to beneficially optimize user cost versus service capabilities or capacities in a manner that facilitates an optimized user experience and does not violate network neutrality goals, regulations and/or requirements. For example, by offering the user with a set of choices, ranging from simple choices between two or more pre-packaged service control settings options to advanced user screens where more detailed level of user specification and control is made

available, some embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, and/or other “entity” to implement valuable or necessary service controls while allowing the user to decide or influence the decision on which service usage activities are controlled, such as how they are controlled or throttled and which service usage activities may not be throttled or controlled in some manner. These various embodiments allow the service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, or other “entity” to assist the user in managing services in a manner that is network neutral with respect to their implementation and service control policies, because the user is making or influencing the decisions, for example, on cost versus service capabilities or quality. By further providing user control or influence on the filtering settings for the service usage reporting or CRM reporting, various levels of service usage and other user information associated with device usage can be transmitted to the network, service provider, device manufacturer, device distributor, MVNO, VSP, service provider partner, and/or other “entity” in a manner specified or influenced by the user to maintain the user’s desired level of information privacy.

[0253] As shown in FIG. 16, the service processor 115 includes the service downloader 1663. In some embodiments, the service downloader 1663 provides a download function to install or update service software elements on the device. In some embodiments, the service downloader 1663 requires a secure signed version of software before a download is accepted. For example, the download can require a unique key for a particular service downloader 1663. As another example, the service downloader 1663 can be stored or execute in secure memory or execute a secure memory partition in the CPU memory space. Those of ordinary skill in the art will appreciate that there are a variety of other security techniques that can be used to ensure the integrity of the service downloader 1663.

[0254] As shown in FIG. 16, the service processor 115 includes a modem driver 1640. In some embodiments, the modem driver 1640 converts data traffic into modem bus (not shown) traffic for one or more modems via the modem firewall 1655. As shown in FIG. 18, in some embodiments, modem selection and control 1811 selects the access network connection and is in communication with the modem firewall 1655, and modem drivers 1831, 1815, 1814, 1813, 1812 convert data traffic into modem bus traffic for one or more modems and are in

communication with the modem selection and control 1811. As shown in FIG. 21, in some embodiments, modems 2141, 2125, 2124, 2123, 2122, which are in communication with the modem bus 2120, connect the device to one or more networks. In some embodiments, different profiles are selected based on the selected network connection (e.g., different service profiles/policies for WWAN, WLAN, WPAN, Ethernet and/or DSL network connections), which is also referred to herein as multimode profile setting. For example, service profile settings can be based on the actual access network (e.g., home DSL/cable or work network) behind the Wi-Fi not the fact that it is Wi-Fi (or any other network, such as DSL/cable, satellite, or T-1), which is viewed as different than accessing a Wi-Fi network at the coffee shop. For example, in a Wi-Fi hotspot situation in which there are a significant number of users on a DSL or T-1 backhaul, the service controller can sit in a service provider cloud or an MVNO cloud, the service controls can be provided by a VSP capability offered by the service provider (e.g., as described herein with respect to FIG. 49) or the service controller can be owned by the hotspot service provider that uses the service controller on their own without any association with an access network service provider. For example, the service processors can be controlled by the service controller to divide up the available bandwidth at the hotspot according to QoS or user sharing rules (e.g., with some users having higher differentiated priority (potentially for higher service payments) than other users). As another example, ambient services (as similarly described herein) can be provided for the hotspot for verified service processors.

[0255] In some embodiments, the service processor 115 and service controller 122 are capable of assigning multiple service profiles associated with multiple service plans that the user chooses individually or in combination as a package. For example, a device 100 starts with ambient services that include free transaction services wherein the user pays for transactions or events rather than the basic service (e.g., a news service, eReader, PND service, pay as you go session Internet) in which each service is supported with a bill by account capability to correctly account for any subsidized partner billing to provide the transaction services (e.g., Barnes and Noble may pay for the eReader service and offer a revenue share to the service provider for any book or magazine transactions purchased from the device 100). In some embodiments, the bill by account service can also track the transactions and, in some embodiments, advertisements for the purpose of revenue sharing, all using the service monitoring capabilities disclosed herein. After initiating services with the free ambient service discussed above, the user may later choose

a post-pay monthly Internet, email and SMS service. In this case, the service controller 122 would obtain from the billing system 123 in the case of network based billing (or in some embodiments the service controller 122 billing event server 1622 in the case of device based billing) the billing plan code for the new Internet, email and SMS service. In some embodiments, this code is cross referenced in a database (e.g., the policy management server 1652) to find the appropriate service profile for the new service in combination with the initial ambient service. The new superset service profile is then applied so that the user maintains free access to the ambient services, and the billing partners continue to subsidize those services, the user also gets access to Internet services and may choose the service control profile (e.g., from one of the embodiments disclosed herein). The superset profile is the profile that provides the combined capabilities of two or more service profiles when the profiles are applied to the same device 100 service processor. In some embodiments, the device 100 (service processor 115) can determine the superset profile rather than the service controller 122 when more than one “stackable” service is selected by the user or otherwise applied to the device. The flexibility of the service processor 115 and service controller 122 embodiments described herein allow for a large variety of service profiles to be defined and applied individually or as a superset to achieve the desired device 100 service features.

[0256] As shown in FIG. 16, the service controller 122 includes a service control server link 1638. In some embodiments, device based service control techniques involving supervision across a network (e.g., on the control plane) are more sophisticated, and for such it is increasingly important to have an efficient and flexible control plane communication link between the device agents (e.g., of the service processor 115) and the network elements (e.g., of the service controller 122) communicating with, controlling, monitoring, or verifying service policy. For example, the communication link between the service control server link 1638 of service controller 122 and the service control device link 1691 of the service processor 115 can provide an efficient and flexible control plane communication link, a service control link 1653 as shown in FIG. 16, and, in some embodiments, this control plane communication link provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the service processor 115 and the service controller 122. In some embodiments, the service control server link 1638 provides the network side of a system for transmission and reception of service agent to/from network element functions. In some

embodiments, the traffic efficiency of this link is enhanced by buffering and framing multiple agent messages in the transmissions (e.g., thereby reducing network chatter). In some embodiments, the traffic efficiency is further improved by controlling the transmission frequency and/or linking the transmission frequency to the rate of service usage or traffic usage. In some embodiments, one or more levels of security and/or encryption are used to secure the link against potential discovery, eavesdropping or compromise of communications on the link. In some embodiments, the service control server link 1638 also provides the communications link and heartbeat timing for the agent heartbeat function. As discussed below, various embodiments described herein for the service control server link 1638 provide an efficient and secure mechanism for transmitting and receiving service policy implementation, control, monitoring and verification information between the device agents (e.g., service processor agents/components) and other network elements (e.g., service controller agents/components).

[0257] In some embodiments, the service control server link 1638 can employ the counterpart service control plane secure transmission methods discussed above with respect to the service control device link 1691. For example, one or more layers of security can be used to secure the communications link, including, for example, basic IP layer security, TCP layer security, service control link layer security, and/or security specific from service controller servers to service processor agents.

[0258] In some embodiments, the service control server link 1638 reduces network chatter by efficiently transmitting service control related communications over the link. For example, the service control server link 1638 can transmit server messages asynchronously as they arrive. As another example, the service control server link 1638 can perform collection or buffering of server messages between transmissions. As another example, the service control server link 1638 can determine when to transmit based potentially on several parameters, such as one or more of: periodic timer trigger, waiting until a certain amount of service usage or traffic usage has occurred, responding to a service agent message, responding to a service agent request, initiated by one or more servers, initiated by a verification error condition, and/or initiated by some other error condition. For example, once a transmission trigger has occurred, the service control server link 1638 can take all buffered agent communications and frame the communications. In addition, the service control server link 1638 can provide for an efficient

communication link based on various embodiments related to the timing of transmissions over the service control link, as similarly discussed above with respect to the service control device link 1691 description. For example, the timing functions, such as asynchronous messages or polling for messages, constant frequency transmission, transmission based on how much service usage or data traffic usage has taken place, transmission in response to device side control link message, service verification error events, other error events, and/or other message transmission trigger criteria can be determined, controlled and/or initiated by either the device side or the network side depending on the embodiment.

[0259] In some embodiments, the service control server link 1638 provides for securing, signing, encrypting and/or otherwise protecting the communications before sending such communications over the service control link 1653. For example, the service control server link 1638 can send to the transport layer or directly to the link layer for transmission. In another example, the service control server link 1638 further secures the communications with transport layer encryption, such as TCP TLS or another secure transport layer protocol. As another example, the service control server link 1638 can encrypt at the link layer, such as using IPSEC, various possible VPN services, other forms of IP layer encryption and/or another link layer encryption technique.

[0260] In some embodiments, the service control server link 1638 includes the agent heartbeat function in which the agents provide certain required reports to the service processor for the purpose of service policy implementation verification or for other purposes. For example, the heartbeat function can also be used to issue queries or challenges, messages, service settings, service control objectives, information requests or polling, error checks and/or other communications to the agents. As another example, agent heartbeat messages can be in the open or encrypted, signed and/or otherwise secured. Additional heartbeat function and the content of heartbeat messages can be provided as similarly described herein, such as described above with respect to the service control device link 1691 and the access control integrity agent 1694 and other sections. In some embodiments, the service controller 122 and/or agents of the service controller 122 are programmed to periodically provide reports, such as upon a heartbeat response (e.g., an agent can repeatedly send necessary reports each heartbeat), and appropriate actions can then be taken based upon such received reports. Accordingly, the heartbeat function

provides an important and efficient system in various embodiments described herein for verifying the service policy implementation and/or protecting against compromise events. There are many other functions the agent heartbeat service can perform many of which are discussed herein, while many others will be apparent to one of ordinary skill in the art given the principles, design background and various embodiments provided herein.

[0261] In some embodiments, the service control server link 1638 also provides a service control software download function for various embodiments, which, for example, can include a download of new service software elements, revisions of service software elements, and/or dynamic refreshes of service software elements of the service processor 115 on the device. In some embodiments, this function is performed by the service control server link 1638 transmitting the service control software as a single file over the service control link. For example, the file can have encryption or signed encryption beyond any provided by the communication link protocol itself for service control link 1653. In another example, the service control software files can be segmented/divided into smaller packets that are transmitted in multiple messages sent over the service control link 1653. In yet another example, the service control software files can be transmitted using other delivery mechanism, such as a direct TCP socket connection from a service download control server 1660, which can also involve secure transport and additional levels of encryption. In some embodiments, the service control server link 1638 and/or service download control server 1660 use(s) an agent serial number and/or a security key look up when agents are updated and/or when a dynamic agent download occurs.

[0262] As shown in FIG. 16, the service controller 122 includes an access control integrity server 1654. In some embodiments, the access control integrity server 1654 collects device information on service policy, service usage, agent configuration and/or agent behavior. For example, the access control integrity server 1654 can cross check this information to identify integrity breaches in the service policy implementation and control system. In another example, the access control integrity server 1654 can initiate action when a service policy violation or a system integrity breach is suspected.

[0263] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) acts on access control integrity agent reports and error

conditions. Many of the access control integrity agent 1654 checks can be accomplished by the server. For example, the access control integrity agent 1654 checks include one or more of the following: service usage measure against usage range consistent with policies (e.g., usage measure from the network and/or from the device); configuration of agents; operation of the agents; and/or dynamic agent download.

[0264] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy implementations by comparing various service usage measures (e.g., based on network monitored information, such as by using IPDRs, and/or local service usage monitoring information) against expected service usage behavior given the policies that are intended to be in place. For example, device service policy implementations can include measuring total data passed, data passed in a period of time, IP addresses, data per IP address, and/or other measures such as location, downloads, email accessed, URLs, and comparing such measures expected service usage behavior given the policies that are intended to be in place.

[0265] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy, and the verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: unauthorized network access (e.g., access beyond ambient service policy limits); unauthorized network speed (e.g., average speed beyond service policy limit); network data amount does not match policy limit (e.g., device not stop at limit without re-up/revising service policy); unauthorized network address; unauthorized service usage (e.g., VOIP, email, and/or web browsing); unauthorized application usage (e.g., email, VOIP, email, and/or web); service usage rate too high for plan, and policy controller not controlling/throttling it down; and/or any other mismatch in service measure and service policy.

[0266] In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy based at least in part on, for example, various error conditions that indicate a mismatch in service measure and service policy. For example, various verification error conditions that can indicate a mismatch in service measure and service policy include one or more of the following: mismatch in one service

measure and another service measure; agent failure to report in; agent failure to respond to queries (e.g., challenge-response sequence and/or expected periodic agent reporting); agent failure to respond correctly to challenge/response sequence; agent improperly configured; agent failure in self checks; agent failure in cross-checks; unauthorized agent communication or attempted unauthorized communication; failure in service policy implementation test; failure in service usage reporting test; failure in service usage billing test; failure in transaction billing test; failure in download sequence; environment compromise event, such as unauthorized software load or execution (or attempt), unauthorized memory access (or attempt), unauthorized agent access (or attempt), known harmful software, and/or known harmful communications signature; and/or failure to respond to various messages, such as send message and suspend and/or send message and quarantine. In some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) verifies device service policy by performing automated queries and analysis, which are then reported (e.g., anomalous/suspicious report results can be reported for further analysis by a person responsible for determining whether such activities indicate out of policy activities or to provide information to the user to inform the user of such anomalous/suspicious report results that may indicate out of policy activities). For example, the user can review the report to authorize whether such activities were performed by the user (e.g., website access requests, specific transactions, and/or phone calls) and/or indicate that such activities were not authorized by the user (e.g., indicate a potential compromise of the device, such as by malware or other unauthorized software/user use of the device). In another example, the user can also be connected to communicate with service support of the service provider regarding such reported activities (e.g., by text/chat, voice/phone, and/or video conference to a service support). Accordingly, in some embodiments, the access control integrity server 1654 (and/or some other agent of service controller 122) provides a policy/service control integrity service to continually (e.g., periodically and/or based on trigger events) verify that the service control of the device has not been compromised and/or is not behaving out of policy.

[0267] In some embodiments, upon detection of one or more service verification errors, such as the various service verification errors discussed above, the device is directed to a quarantine network status in which the device can, for example, only access network control plane functions, billing functions, and other functions generally controlled by the access network

service provider or the central service provider. For example, quarantine network access restrictions and routing can be accomplished with the access network AAA and routing system (e.g., access network AAA server 1621 and one or more of the gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720) or can be accomplished with device based access control or traffic control policy implementation. Quarantine network equipment or servers can, for example, be located within the access network or within another network with access to the access network. Communication with the quarantine network infrastructure can be accomplished, for example, with a secure link with one or more encryption levels or a dedicated private link. In some embodiments, quarantining a device includes, for example, a two step process for routing quarantine network device traffic, first, to a quarantine traffic handling router or server and, second, from there to the actual quarantine network infrastructure, with the route being determined by device parameters, user parameters, access service provider parameters or other parameters associated with the quarantine network routing. In some embodiments, the device is completely suspended from the network in which, for example, the device can first issue a user interface message to the user or issuing another form of a message to the user or service subscriber, such as via email, hard copy message and/or voice message. In some embodiments, the device network access, service capabilities and/or traffic shaping are limited, partially restricted or completely restricted, service capabilities. For example, these limitations and/or restrictions can be implemented in the device and/or in the network. For example, implementing a device quarantine (e.g., using a RADIUS server to quarantine the device) can involve assigning the device to a different billing profile.

[0268] In some embodiments, upon detection of one or more service verification errors, such as the various service verification errors discussed above, switch based port analysis is performed to further monitor the device (e.g., referred to as Switched Port Analyzer (SPAN) on Cisco switches, and various other vendors have different names for it, such as Roving Analysis Port (RAP) on 3Com switches). In some embodiments, the device service policy implementation behavior is monitored at a deeper level in the network by copying device traffic in the switch so that it goes to both an intended data path destination and to a specified port for switch based port analysis (e.g., the traffic content can be analyzed and recorded using deep packet inspection (DPI) techniques, which can provide a finer level of detail than the typical IPDR). For example, an advantage of performing a switch based port analysis function is that

the traffic need not be analyzed in real time, and a sample subset of the devices on the network can be selected for such analysis based on, for example, either identifying devices that have suspect service policy implementation behavior and/or a regular sampling algorithm that eventually samples all devices, or some other selection approaches. As another example, a scheduled switch based port analysis sampling can be applied that eventually rotates through all devices and designates a higher priority in the sampling queue for devices that are suspect.

[0269] In some embodiments, switch based port analysis allows for off-line sampled or non-real-time DPI, as described above, as a verification measure for the device based service control measures that are implemented. In some embodiments, sophisticated DPI techniques are used to enhance the content of the IPDRs so that they provide detailed information that can be made available in the network. For example, some of the DPI packet analysis may be redundant between the device and the network, but this approach provides for a much finer grain validation for the device based service and less reliance on the device for some of the service traffic analysis that service providers need. In some embodiments, the device control server functions and the service control policy verification functions are implemented in an integrated hardware/software system (e.g., a gateway, server, router, switch, base station, base station aggregator, AAA server cluster or any other hardware or hardware/software system) located in the network that the network level traffic inspection is accomplished in, or in one or more servers integrated to operate in a coordinated manner with the DPI boxes. In some embodiments, the device control server functions and the service control policy verification functions are implemented in an integrated hardware/software system (e.g., a gateway, server, router, switch, base station, base station aggregator, AAA server cluster or any other hardware or hardware/software system) located in the network that provides deep service control capability (e.g., using DPI techniques) for devices that have some or all of the service processor functions installed and, in some embodiments, also providing coarser network control of the basics for devices that do not have a service processor installed in the device (e.g., such coarser network control functions include max data rate and/or max total data).

[0270] In some embodiments, the SPAN function is used in a revolving periodic manner as well to augment CDR data with deeper packet information for the purpose of spot-checking device based service usage measures. Examples of where this can be beneficial include spot

checking network address access policies, spot checking ambient access policies, spot checking billing event reports, spot checking intermediate networking device/end point device count (via checking network source or destination addresses, token, cookies or other credentials, etc). For example, the periodic SPAN can be scheduled for all devices equally, for certain devices or users with higher priority, frequency or depth of SPAN than others, higher priority, higher frequency or immediate priority for devices with higher usage patterns or unusual usage patterns, immediate or very high priority for devices with a policy violation status.

[0271] In some embodiments, a combination traffic inspection and service control approach implements traffic and service control functions in the network that are conducive for a network based implementation and implements traffic and service control functions in the device that are either more conducive for performing in the device or can only be performed in the device (e.g., activities involving inspection of traffic that is encrypted once it is transmitted to the network). For example, using this approach, activities that can be done in the network are generally performed in the network and/or are more efficiently performed in the network than the device, and activities that are more efficiently performed in the device or can only be performed in the device are performed in the device (e.g., depending on device processing/storage capabilities and/or other design/security considerations). For example, the following are various traffic and service control functions that, in some embodiments, are preferably or can only be performed in the device: network based packet processing capability limitations (e.g., encrypted traffic, application layer information unavailable once the traffic goes into the networking stack, other application/usage context information available on the device but not in the network); information that is generally/preferably maintained and processed locally in the device for network neutrality reasons (e.g., network neutrality issues can generally be efficiently implemented by keeping all, substantially all or at least some aspect of decisions on how to implement algorithms to control traffic local to the device and under user decision control, and/or by providing the user with a set of pre-packaged choices on how to manage service usage or service activity usage or manage service usage versus service cost or price); information that is generally/preferably maintained and processed locally in the device for user privacy reasons (e.g., deeper levels of traffic monitoring and service usage monitoring data where it is available for assisting the user in achieving the best, lowest cost experience and implementing a CRM filter function to the user so that the user can control the level of CRM the network is allowed to

receive, such as with the higher levels of information being exchanged for something of value to the user, and/or user location information); information that is generally/preferably maintained and processed locally in the device for the purpose of informing the user of service control settings or service activity usage or to adjust service activity control settings or receive user feedback to choices regarding service usage policies or billing options (e.g., providing the user with a UI for the purpose of monitoring an estimate of service usage and/or notifying the user of at least some aspect of estimated service usage or projected service usage, providing the user with a UI for the purpose of monitoring an estimate of service cost and/or notifying the user of at least some aspect of estimated service cost or projected service cost, providing the user with a UI for the purpose of providing the user with one or more service usage and/or service cost notification messages that require user acknowledgement and/or a user decision and obtaining or reporting the user acknowledgements and/or decisions, providing the user with a UI for the purpose of providing the user with service options and/or service payment options, providing the user with a UI for the purpose of obtaining user choice for such options when service usage or cost estimates are about to run over limits or have run over limits or are projected to run over limits, providing the user with a UI for the purpose of monitoring or conducting open central billing transactions or other transactions, providing the user with a UI for the purpose of selecting the service control techniques and/or policies and/or algorithms and/or pre-packaged configurations that can be used to define or partially define the service activity usage control policies implemented in the device service processor or the network service control equipment/billing system or a combination of both); service control for roaming on different networks that typically do not have compatible DPI-type techniques with the home network; certain service notification and traffic control algorithms (e.g., stack-ranked activity statistical analysis and control of only the high usage activities); and/or a function for assigning a device to a service experience or ambient activation experience or virtual service provider (VSP) at various times from manufacturing to device distribution to a user of the device. In some embodiments, certain activities are implemented in the device as a solution for networks in which a new centralized DPI approach is not possible, not economically feasible, or for any number of reasons not an option or not a preferred option.

[0272] In some embodiments, a network based solution is provided for a more basic set of services for all devices that do not have service control capabilities, and a super-set of services

and/or additional services are provided for devices that include a service processor. As described herein, a service controller function can be located in various places in the network in accordance with various embodiments. It should also be noted that various other embodiments described herein also employ a hybrid service control function performing certain service control functions in the network (e.g., collecting network service usage information, such as IPDRs, and/or performing DPI related functions in the network for collecting network service usage information and/or throttling/shaping traffic) and service control functions in the device (e.g., service processor 115, which, for example, monitors service usage in the device and/or performs throttling or traffic shaping in the device and/or performs certain billing event recording and reporting functions that are aptly performed on the device).

[0273] In some embodiments, lower level service policy implementation embodiments are combined with a higher level set of service policy supervision functions to provide device assisted verifiable network access control, authentication and authorization services.

[0274] In some embodiments, device based access control services are extended and combined with other policy design techniques to create a simplified device activation process and connected user experience referred to herein as ambient activation. As similarly discussed above, ambient activation can be provided by setting access control to a fixed destination, verifying access with IPDRs, verifying access by setting a max data rate and triggering off in the network if it exceeds the max data rate, and/or by various other techniques.

[0275] As shown in FIG. 16, service controller 122 includes a service history server 1650. In some embodiments, the service history server 1650 collects and records service usage or service activity reports from the Access Network AAA Server 1621 and the Service Monitor Agent 1696. For example, although service usage history from the network elements can in certain embodiments be less detailed than service history from the device, the service history from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is extremely difficult for a device error or compromise event on the device to compromise the network based equipment and software. For example, service history reports from the device can include various service tracking information, as similarly described above. In some embodiments, the service history server 1650 provides the

service history on request to other servers and/or one or more agents. In some embodiments, the service history server 1650 provides the service usage history to the device service history 1618. In some embodiments, for purposes of facilitating the activation tracking service functions (described below), the service history server 1650 maintains a history of which networks the device has connected to. For example, this network activity summary can include a summary of the networks accessed, activity versus time per connection, and/or traffic versus time per connection. As another example, this activity summary can further be analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.

[0276] As shown in FIG. 16, service controller 122 includes a policy management server 1652. In some embodiments, the policy management server 1652 transmits policies to the service processor 115 via the service control link 1653. In some embodiments, the policy management server 1652 manages policy settings on the device (e.g., various policy settings as described herein with respect to various embodiments) in accordance with a device service profile. In some embodiments, the policy management server 1652 sets instantaneous policies on policy implementation agents (e.g., policy implementation agent 1690). For example, the policy management server 1652 can issue policy settings, monitor service usage and, if necessary, modify policy settings. For example, in the case of a user who prefers for the network to manage their service usage costs, or in the case of any adaptive policy management needs, the policy management server 1652 can maintain a relatively high frequency of communication with the device to collect traffic and/or service measures and issue new policy settings. In this example, device monitored service measures and any user service policy preference changes are reported, periodically and/or based on various triggers/events/requests, to the policy management server 1652. In this example, user privacy settings generally require secure communication with the network (e.g., a secure service control link 1653), such as with the policy management server 1652, to ensure that various aspects of user privacy are properly maintained during such configuration requests/policy settings transmitted over the network. For example, information can be compartmentalized to service policy management and not communicated to other databases used for CRM for maintaining user privacy.

[0277] In some embodiments, the policy management server 1652 provides adaptive policy management on the device. For example, the policy management server 1652 can issue policy settings and objectives and rely on the device based policy management (e.g., service processor 115) for some or all of the policy adaptation. This approach can require less interaction with the device thereby reducing network chatter on service control link 1653 for purposes of device policy management (e.g., network chatter is reduced relative to various server/network based policy management approaches described above). This approach can also provide robust user privacy embodiments by allowing the user to configure the device policy for user privacy preferences/settings so that, for example, sensitive information (e.g., geo-location data, website history) is not communicated to the network without the user's approval. In some embodiments, the policy management server 1652 adjusts service policy based on time of day. In some embodiments, the policy management server 1652 receives, requests or otherwise obtains a measure of network availability and adjusts traffic shaping policy and/or other policy settings based on available network capacity.

[0278] In some embodiments, the policy management server 1652 performs a service control algorithm to assist in managing overall network capacity or application QoS. In some embodiments, the policy management server 1652 performs an algorithm to determine which access network is best to connect to, such as based on network capacity or application QoS, service usage costs, and/or any other criteria. In some embodiments, the device is capable of connecting to more than one network, and accordingly, device service policies can be selected/modified based on which network the device is connected to. In some embodiments, the network control plane servers detect a network connection change from a first network to a second network and initiate the service policy implementation established for the second network. In other embodiments, the device based adaptive policy control agent (e.g., policy control agent 1692 described herein) detects network connection changes from the first network to the second network and implements the service policies established for the second network.

[0279] In some embodiments, when more than one access network is available, the network is chosen based on which network is most preferred according to a network preference list or according to the network that optimizes a network cost function. For example, the preference list can be pre-established by the service provide and/or the user. For example, the

network cost function can be based on a minimum service cost, maximum network performance, determining whether or not the user or device has access to the network, maximizing service provider connection benefit, reducing connections to alternative paid service providers, and/or a variety of other network preference criteria. In other embodiments, the device detects when one or more preferred networks are not available, implements a network selection function or intercepts other network selection functions, and offers a connection to the available service network that is highest on a preference list. For example, the preference list can be set by the service provider, the user and/or the service subscriber.

[0280] As shown in FIG. 16, service controller 122 includes a network traffic analysis server 1656. In some embodiments, the network traffic analysis server 1656 collects/receives service usage history for devices and/or groups of devices and analyzes the service usage. In some embodiments, the network traffic analysis server 1656 presents service usage statistics in various formats to identify improvements in network service quality and/or service profitability. In other embodiments, the network traffic analysis server 1656 estimates the service quality and/or service usage for the network under variable settings on potential service policy. In other embodiments, the network traffic analysis server 1656 identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.

[0281] As shown in FIG. 16, service controller 122 includes a beta test server 1658. In some embodiments, the beta test server 1658 publishes candidate service plan policy settings to one or more devices. In some embodiments, the beta test server 1658 provides summary reports of network service usage or user feedback information for one or more candidate service plan policy settings. In some embodiments, the beta test server 1658 provides a mechanism to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further policy settings optimization.

[0282] As shown in FIG. 16, service controller 122 includes a service download control server 1660. In some embodiments, the service download control server 1660 provides a download function to install and/or update service software elements (e.g., the service processor 115 and/or agents/components of the service processor 115) on the device, as described herein.

[0283] As shown in FIG. 16, service controller 122 includes a billing event server 1662. In some embodiments, the billing event server 1662 collects billing events, provides service plan information to the service processor 115, provides service usage updates to the service processor 115, serves as interface between device and central billing server 1619, and/or provides trusted third party function for certain ecommerce billing transactions.

[0284] As shown in FIG. 16, the Access Network AAA server 1621 is in network communication with the access network 1610. In some embodiments, the Access Network AAA server 1621 provides the necessary access network AAA services (e.g., access control and authorization functions for the device access layer) to allow the devices onto the central provider access network and the service provider network. In some embodiments, another layer of access control is required for the device to gain access to other networks, such as the Internet, a corporate network and/or a machine to machine network. This additional layer of access control can be implemented, for example, by the service processor 115 on the device. In some embodiments, the Access Network AAA server 1621 also provides the ability to suspend service for a device and resume service for a device based on communications received from the service controller 122. In some embodiments, the Access Network AAA server 1621 also provides the ability to direct routing for device traffic to a quarantine network or to restrict or limit network access when a device quarantine condition is invoked. In some embodiments, the Access Network AAA server 1621 also records and reports device network service usage (e.g., device network service usage can be reported to device service history 1618).

[0285] As shown in FIG. 16, the device service history 1618 is in network communication with the access network 1610. In some embodiments, the device service history 1618 provides service usage data records used for various purposes in various embodiments. In some embodiments, the device service history 1618 is used to assist in verifying service policy implementation. In some embodiments, the device service history 1618 is used to verify service monitoring. In some embodiments, the device service history 1618 is used to verify billing records and/or billing policy implementation. In some embodiments, the device service history 1618 is used to synchronize and/or verify the local service usage counter.

[0286] As shown in FIG. 16, the central provider billing server 1619 is in network communication with the access network 1610. In some embodiments, the central provider billing server 1619 provides a mediation function for central provider billing events. For example, the central provider billing server 1619 can accept service plan changes. In some embodiments, the central provider billing server 1619 provides updates on device service usage, service plan limits and/or service policies. In some embodiments, the central provider billing server 1619 collects billing events, formulates bills, bills service users, provides certain billing event data and service plan information to the service controller 122 and/or device 100.

[0287] Establishing Coordinated Service and Verification Policies for Service Processor, Service Controller and Network Functions

[0288] In some embodiments, device and network apparatus coordinate one or more of the following: network service policy implementation settings, device service policy implementation settings, network service profile implementation settings, device service profile implementation settings, network service usage measures used for the purpose of verifying service policy implementation, device service usage measures used for the purpose of verifying service policy implementation, network actions taken upon detection of service usage policy violation and device actions taken upon detection of service usage policy violation. In some embodiments, local device settings for the service monitoring, usage and/or billing profile or policy settings used, for example, by a device service processor 115, are associated with corresponding records for the various network apparatus that also rely upon the service policy and profile settings to monitor, control and/or bill for services or to respond to out of policy service usage conditions. For example, such network apparatus include the service controller 122 or similar functions, the billing system 123 or similar functions, the network AAA 121, gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720, or other networking equipment. In some embodiments, the service profile or policy settings are associated between the device and network in a manner that allows for effective and coordinated operation between the device service processor 115 and the network apparatus, but does not require an explicit function that simultaneously controls/ coordinates the service policy or profile implementation and/or verification actions taken by the device 100 (e.g., the service processor 115) and the network

apparatus. As an example, such embodiments can be applied in overlay applications as discussed below.

[0289] In some embodiments, a network function (e.g., the service controller 122, and/or more specifically the policy management server 1652 function, or other similar function) obtain, derive or otherwise determine the association of the service profile or policy settings to program a device service processor 115 and the various network apparatus functions (e.g., possibly including but not limited to the service controller 122 or similar functions, the billing system 123 or similar functions, the network AAA 121, gateways 410, 420, 508, 512, 520, 608, 612, 620, 708, 712, 720, or other networking equipment) by reading, receiving, querying, pulling or otherwise obtaining the settings from one or more of the network apparatus functions or from a data base that stores the service policy or profile settings for one or more of the network apparatus functions. After obtaining one or more of the network apparatus settings, a mapping (e.g., an association) of the network apparatus settings to the appropriate device 100 (service processor 115) settings can be determined to advantageously support the service usage monitoring, service usage control, service usage billing or service usage verification objectives being addressed. The policy or profile settings for the device can be a direct translation of the policy or profile settings used for the network apparatus, or the device policy or profile settings can be less directly derived from the network apparatus policy or profile settings. For example, service usage limits contained in the billing system 123 service plan can be either directly mapped to usage limit settings on the device service processor 115 (e.g., service usage stops when the limit is hit or the user is notified or the user is billed), or the usage limits can be mapped to a number of service profiles the user may select from (e.g., as discussed herein, the user can select from options involving various actual usage versus usage limit notification policies and/or service usage control, limitations or throttling policies).

[0290] For example, the service usage policy or profile limits or allowances maintained for the network apparatus functions (e.g., the service profile or service plan usage limits stored in the billing system 123 or AAA 121) can be read or queried by a network function (e.g., the service controller 122 or the service controller 122 through a second intermediary server connected to the billing system 123 and/or the AAA system 121), and the service usage limits stored in these networking apparatus can be either directly translated to the settings for the

service processor 115 or may need to be interpreted, expanded or otherwise modified to obtain the required service processor 115 policy and/or profile settings.

[0291] In some embodiments, the service usage limits set in the billing system 123 service plan record, and/or the service profile record stored in the AAA system 121 can be acquired (e.g., from the apparatus or from a database storing the settings for the apparatus) by the service controller (or another network function) and directly translated and used to program the settings in the service processor 123. In some embodiments, the service usage limits are determined or obtained by the activation server apparatus embodiments, other apparatus embodiments associated with service activation, or the virtual service provider embodiments, as described herein. In this manner, once the association of the service usage profile or policy settings used by a device service processor 115 and the profile or policy settings used by the various network apparatus functions is established, then the service policy or profile for service monitoring, control, billing, verification and/or actions taken on verification error can be coordinated between device and network even if some of the network functions act independent of some of the device functions.

[0292] For example, associating the service usage policies and/or profiles between the device service processor 115 and the various network apparatus functions, and then allowing for independent operation or action by the various functions in a manner that results in a coordinated outcome, facilitates an overlay of the device assisted services technology onto existing network equipment in a manner that results in reliable and verifiable service enhancements while minimizing the need for major existing network equipment upgrades.

[0293] In some embodiments, the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings used by the various network apparatus functions can be provided by a centralized network function that determines the appropriate settings for the network apparatus and the service processor 115 and sets one or more settings to each function. In some embodiments, this networking function is provided by a centralized network management function or service account activation function (e.g., the activation server apparatus embodiments, one of the other disclosed apparatus

embodiments associated with service activation or the virtual service provider apparatus embodiments, as described herein).

[0294] In some embodiments, the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings used by the various network apparatus functions can be provided by a network function that by reads, receives, queries, pulls or otherwise obtains the setting used by the service controller 122 or the service processor 115. The network function can then determine the association of the service profile or policy settings used by a device service processor 115 and the service profile or policy settings required by the various network apparatus functions before writing, transmitting, pushing, or otherwise recording the appropriate settings required by each of the other network apparatus functions. In some embodiments, this functionality can be implemented in the service controller (e.g., the policy management server, possibly acting in coordination with another network function or server), which then links into the databases used for storing the policy or profile settings for the other network apparatus.

[0295] In some embodiments, once the association is established between service policy or profile settings in the network apparatus and the service policy or profile settings in the service processor 115, then the network based service usage measures (e.g., IPDRs communicated to the billing system 123, the AAA 121, service controller 122 or other network functions used to verify service usage and/or take actions) used for verification of device 100 service usage versus service policy or profile can be monitored by the network apparatus (e.g., billing system 123 and AAA 121) independent of coordination with the service processor 115 and/or independent of the service controller 122. In some embodiments, in addition to independent monitoring and verification of service usage versus policy, independent service profile or policy verification error response actions can be taken by the network apparatus (e.g., suspend, quarantine, SPAN or flag device 100, notify the user and possibly require acknowledgement, or bill the user account for service usage overage) without direct involvement by the service processor 115 and/or the service controller 122.

[0296] Accordingly, the association between service profile and/or service policy that is implemented on the device 100 (e.g., service processor 115) and the service profile and/or policy

usage limits recorded in network apparatus can be associated with one another by one or more of the following: (A) implementing a function to read from the network database (e.g., the billing 123 data base, AAA 121 data base, service controller 122 data base, etc.) and mapping the network profiles and/or policies to device 100 (e.g., service processor 115) profiles and/or policies; (B) implementing a function that simultaneously sets the device profile and/or policy and the network equipment profile and/or policy recorded in the appropriate data base records; and (C) implementing a function that reads the profile and/or policy on the device 100 (e.g., service processor 115) or the service controller 122 and then sets the network equipment profile and/or policy recorded in the appropriate data base records. This allows for a simplified but coordinated response to monitoring, controlling and billing for service usage, for verifying service usage versus service usage profile or policy, and/or initiating or carrying out network actions in response to service usage versus profile or policy verification errors and/or device actions in response to service usage versus profile or policy verification errors.

[0297] FIG. 17 is another functional diagram illustrating the device based service processor 115 and the service controller 122 in accordance with some embodiments. FIG. 17 provides for various embodiments as similarly described above with respect to the various embodiments described above with respect to FIG. 16, with one of the differences being that the service controller 122 as shown in FIG. 17 is connected to the access network and not (directly) connected to the Internet. Accordingly, as shown in FIG. 17, in some embodiments, the service control link 1653 is a communications link between the service controller 122 and the service processor 115 over the access network 1610.

[0298] FIG. 18 is another functional diagram illustrating the device based service processor 115 and the service controller 122 in which the service processor controls the policy implementation for multiple access network modems and technologies in accordance with some embodiments. As shown, FIG. 18 provides for various embodiments as similarly described above with respect to the various embodiments described above with respect to FIG. 16, with one of the differences being that the service processor controls the policy implementation for multiple access network modems and technologies. Accordingly, as shown in FIG. 18, in some embodiments, a connection manager 1804, which as shown is in control plane communication with a modem selection and control 1811, provides a control and supervision function for one or

more modem drivers or modems that connect to an access network. In some embodiments, the modem selection and control 1811 selects the access network connection and is in communication with the modem firewall 1655, and modem drivers, which as shown include Dial/DSL modem driver 1831, Ethernet modem driver 1815, WPAN modem driver 1814, WLAN modem driver 1813, and WWAN modem driver 1812, convert data traffic into modem bus traffic for one or more modems and are in communication with the modem selection and control 1811.

[0299] FIG. 19 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. As shown in FIG. 19, a stripped down (e.g., reduced set of agents/components/functionality) embodiment of the service processor 115 and the service controller 122 are provided in which service policy is not adaptive but rather is set by the service controller 122. In this example, the agent within the service processor 115 that implements service policy is the policy implementation agent 1690. Also, in this example, the service controller 122 is similarly stripped down to a simplified configuration (e.g., reduced set of agents/components/functionality).

[0300] Referring to FIG. 19, in some embodiments, many of the service policy implementation verification and compromise protection techniques are similarly provided using these simplified configurations of the service processor 115 and the service controller 122, as described above with respect to, for example, FIG. 16. For example, the service control device link 1691 and service control server link 1638 can be used for downloading service policies to the policy implementation agent 1690 (but, in some embodiments, cannot perform the heartbeat or authentication function).

[0301] For example, a basic service profile or service policy implementation verification technique for this reduced configuration calls for the access control integrity server 1654 to obtain IPDRs from access network AAA server 1621 (or 121) (e.g., or other network functions as described herein) and compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the access control integrity server 1654 initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed

herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0302] In some embodiments, a service profile or service policy implementation verification technique for this reduced configuration calls for the billing system 123 to obtain IPDRs from access network AAA server 1621 (or 121) (or other network functions as discussed herein) and compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the billing system 123 initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0303] In some embodiments, a service profile or service policy implementation verification technique for this reduced configuration calls for the AAA server 1621 (or 121) itself to compare the service usage exhibited by device 100 with a range of expected service usage that would be expected if the intended service policies were in place on the device. In some embodiments, the AAA server 1621 (or 121) initiates or carries out one or more of the service usage profile or policy verification error response actions disclosed herein, including, for example, one or more of the following: notify the user of the out of policy or overage condition, require the user to acknowledge the condition and/or acknowledge a subsequent billing event to proceed, bill the user for service overage, suspend the device from the network, quarantine the device, SPAN the device, or notify a network manager or device management or error handling function.

[0304] Accordingly, this approach provides a basic first layer of service policy implementation verification that does not depend on device based agent behavior for the verification. If the service policy is in error in a way that violates the expected service policy usage limits, then the access control integrity server 1654 will detect this condition and appropriate action can be taken. In some embodiments, if one or more service policy integrity verification tests fail, the appropriate responsive actions can include routing the device to quarantine status, sending an error message to the device or device user interface and then suspend access for the device, and/or limiting access in some way without completely suspending access, as similarly described above. In some embodiments, if one or more service policy integrity verification tests fail, the appropriate responsive actions can include logging excess service usage above the intended service policy limits and billing the user for some or all of the excess usage, sending the user a notification and/or acknowledgement response request (possibly including a simple keystroke acknowledgement, or a password, a biometric signature or other secure response), and/or limiting access in some way without completely suspending access, as similarly described above.

[0305] In some embodiments, a billing system technique provides another verification overlay. For example, the service processor 115 can have a set of service policy implementations (or service profile) that calls for maintaining service usage within a certain limit, or assisting the user or network to maintain service usage to that limit. The billing system 123 can be implemented in a way to provide a “back stop” to the service usage controls or limits provided for by the service processor 115, so that even if the service processor 115 is compromised, hacked, spoofed or is otherwise in error, the billing system 123 protects the service provider, “service owner”, carrier, VSP or network operator from unpaid access beyond the service limits. This can be accomplished, for example, by assigning a service usage limit within the billing system 123 so that if the service processor 115 is compromised and the service usage runs over the desired limit, the billing system 123 automatically charges the user account for the overage. The billing system 123 can receive service usage information from the IPDRs that are aggregated in the network as in the case of a conventional billing system, and because these network based measures are independent from the device agent operation, they cannot be spoofed by merely spoofing something on the device or service processor 115. In this manner, defeating the service processor 115 service agent control mechanisms described herein simply

results in a billing charge and not free service. In some embodiments, if the service usage runs over the service usage limit specified in the service profile, the user can be notified as discussed herein, and the user can be required to acknowledge the overage and approve a billing charge for the overage as also discussed herein, with the acknowledgement being communicated back to the network in some embodiments. This positive acknowledgement also provides a layer of protection and verification of the service control and usage limit control for the device service processor 115. In some embodiment also discussed herein, the user is requested to input a password, biometric or other secure response to the usage overage notification, providing yet another layer of protection to verify that the user intends to pay for the service usage overage. In these embodiments taken individually or in combination, the service processor 115 assistance for service usage control can be verified and/or protected from compromise.

[0306] In some embodiments, the service control device link 1691 and service control server link 1638 are used to implement the service processor 115 heartbeat authentication and communication functions to strengthen the verification of a proper service policy implementation of the embodiments of FIG. 19. For example, the heartbeat function can be used as authentication for service monitoring versus network reports. In addition, the heartbeat function can be used as authentication for challenge/response queries of agents. Also, the heartbeat function can be used as authentication for access control. In some embodiments, to strengthen verification of the basic system illustrated in FIG. 19, the communication access to the policy implementation agent 1690 is restricted so that software or hardware on device 100 and/or on a network cannot have authorized access to the policy implementation agent 1690. For example, authorized access to the policy implementation agent 1690 can be restricted to include only the service controller 122 through the service control device link 1691 and the service control server link 1638. For example, the agent control bus 1630 can be secured with encryption and/or other security techniques so that only the service control device link 1691 can have authorized access to the policy implementation agent 1690. As another example, the agent level message encryption can be used as described herein.

[0307] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened against errors, intrusion, tampering, hacking and/or other inadvertent or intentional integrity degradation by using various other techniques.

For example, the dynamic agent download feature of the service controller 122 can download a new version of the policy implementation agent 1690. In this example, the new agent code can be identical in functionality and also hashed, obfuscated or ordered differently before signing and encryption so that any hacking attempt must be reinitiated, and this process can be periodically repeated or repeated upon a triggering event. Additionally, once the new dynamically loaded agent is in place, it can be required to perform an environment scan to determine if the system configuration or operation are as expected, and/or it can seek to detect elements in the execution environment that can be harmful or threatening to the integrity of the policy implementation. The agent can also be required to report back on the scan within a relatively short period of time so that any attempt to compromise the agent does not have sufficient time to be effective.

[0308] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened to protect the policy implementation from compromise attempts by locating the software and/or hardware used onto an access modem associated with the service. For example, the modem can make it difficult to get access to the policy implementation agent 1690 by employing one or more security elements on one or more access ports into the modem, such as the device bus, an I/O port, a network connection or the debug port. The modem can also store and/or execute the policy implementation agent in secure memory. The modem can also require a secure download key or a secure software signature to accept any updates to the agent software.

[0309] In some embodiments, the service policy implementation agent 1690 of the embodiments of FIG. 19 can be further strengthened against compromise attempts by performing scans of the device 100 code execution environment and/or code storage environment to identify potentially malicious and/or unwanted/untrusted software or hardware. For example, this function can be performed by the policy implementation agent 1690. The agent can have a local database of potentially malicious elements and compare the entries in the database against the elements detected locally using various malicious code, behavior blocking, intrusion detection, and/or other well known techniques for security analysis. Alternatively or in addition, the agent can communicate a list of some or all of the elements detected locally to the service controller 122 to augment or take the place of the database comparison function that can be performed locally, thereby performing such or further such security analysis on the network (e.g., by the

service controller 122), and, in some embodiments, if not automatically detected, such elements detected locally (e.g., and/or samples of such detected potentially malicious code or logs of potentially malicious/suspicious behavior/intrusions) forwarded to security analysts for the service provider for further security analysis (e.g., service provider security analysts and/or an outside security vendor engaged to protect the service provider's network and supported devices). In some embodiments, the agent detects new software downloads, installs and/or invocations and immediately issues an error flag report when potentially malicious software is downloaded, installed or invoked (e.g., file and network based on access security detection techniques). In some embodiments, the agent scans the local software loading and invocation activity along with a log of other software runtime events and regularly reports this trace so that when an error or compromise event occurs the trace preceding the event can be analyzed to determine the offending software or activity trace that took place to cause the compromise or error. For example, once the software or activity that caused the compromise is known or otherwise detected, it can be entered into a refreshed version of the database that the device and other devices use to detect potentially malicious precursor conditions. Examples of such precursor events can include software invocations, software downloads, a sequence of memory I/O events, a sequence of software access events, a sequence of network address or URL communications or downloads, or a sequence of access modem I/O activity.

[0310] FIG. 20 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. As shown in FIG. 20, the modem firewall 1655 has been removed, and firewall and access control and traffic shaping functions are performed in these embodiments by the policy implementation agent 1690 and application interface agent 1693.

[0311] FIG. 21 is another functional diagram illustrating the service processor 115 and the service controller 122 in accordance with some embodiments. FIG. 21 illustrates the various modem drivers and modems 2122 through 2125 and 2141. In some embodiments, the modems, which include WWAN modem 2122, WLAN modem 2123, WPAN modem 2124, Ethernet modem 2125, and Dial/DSL modem 2141, which are in communication with the modem bus 2120, connect the device to one or more networks. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent

1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation agent 1690, or, in some embodiments, the modem firewall agent 1655 or the application interface agent 1693, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult or impossible to make a complete determination of traffic parameters. It should be noted that although the present invention does not need to implement any or all of the measurement points illustrated in FIG. 21 to have an effective implementation as was similarly shown with respect to FIG. 19, various embodiments benefit from these and/or similar measurement points. It should also be noted that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation.

[0312] As shown in FIG. 21, measurement point I occurs at the application interface agent 1693 interface to the applications. At this measurement point, the application traffic can be monitored before it is framed, packetized or encrypted by the lower layers of the networking stack. For example, this allows inspection, characterization, tagging (literal or virtual) and, in some embodiments, shaping or control of services or traffic. At this measurement point, traffic can be more readily associated with applications, URLs or IP addresses, content type, service type, and other higher level parameters. For example, at this level email traffic and downloads, web browser applications and end points, media file transfers, application traffic demand, URL traffic demand and other such service monitoring parameters are more readily observed (e.g., accessible in the clear without the need for deep packet inspection and/or decryption), recorded and possibly shaped or controlled. As described herein, it is also possible to monitor upstream traffic demand at this point and compare it to the other measurement points to determine if the traffic policies in place are meeting overall traffic control policy objectives or to determine if traffic policy implementation is operating properly. For example, the downstream delivered traffic can be optimally observed at this measurement point.

[0313] As shown in FIG. 21, traffic measurement points II and III are situated on the upstream and downstream sides of policy implementation agent 1690. As described herein, these two locations allow potential tracking of upstream and downstream traffic through the stack portions associated with the policy implementation agent 1690. These two locations also provide for potential cross-checking of how the policy implementation agent 1690 is impacting the demand and delivery of traffic. In a similar manner, measurement point III in connection with measurement point IV provide an opportunity for packet tracing through the stack components associated with the modem firewall 1655 and provide for the opportunity to observe the demand and delivery sides of the modem firewall 1655. Traffic measurement point V provides the potential for observing the traffic at the modem bus drivers for each of the modems.

[0314] As shown in FIG. 21, traffic measurement point VI provides, in some embodiments, the ultimate measure of access traffic, for example, the traffic that actually transacts over the access network through the modem. As shown, measurement point VI is at the modem side of the internal or external communications bus 1630, and it will be appreciated that, in some embodiments, this measurement point can be further down the modem stack closer to the MAC or physical layer (e.g., at the designer's discretion). An advantage of having a measurement point deep in the modem is, for example, that if the software or hardware that implements the measurement and reporting is well secured against compromise, then this measure can be almost as strong from a verification perspective as the measure that comes from the network (e.g., from the network elements). Accordingly, this makes it possible to compare this measure against the other measures to determine if there is a traffic path that is leaking past the other measurement point or one or more policy implementation points.

[0315] FIGS. 22A and 22B provide tables summarizing various service processor 115 agents (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments. Many of these agents are similarly described above, and the tables shown in FIGS. 22A and 22B are not intended to be an exhaustive summary of these agents, nor an exhaustive description of all functions that the agents perform or are described herein, but rather FIGS. 22A and 22B are provided as a summary aid in understanding the basic functions of each agent in accordance with some embodiments and how the agents interact with one another,

with the service controller server elements, and/or with other network functions in certain embodiments to form a reliable device based service delivery solution and/or platform.

[0316] FIG. 23 provides a table summarizing various service controller 122 server elements (and/or components/functions implemented in software and/or hardware) in accordance with some embodiments. Many of these agents are similarly described above, and the table shown in FIG. 23 is not intended to be an exhaustive summary of these server elements, nor an exhaustive description of all functions that the elements perform or are described herein, but rather FIG. 23 is provided as a summary aid in understanding the basic functions of each element in accordance with some embodiments and how the elements interact with one another, certain network elements, and/or the service processor agents in certain embodiments to form a reliable device based service delivery solution and/or platform.

[0317] In some embodiments, it is desirable to provide a control plane between the service processor and the service controller using a flexible connection or communication path that, for example, will work between virtually any two network connection endpoints, one being the service controller and one being the device, in a secure yet scalable manner. In view of the embodiments described herein, one of ordinary skill in the art will recognize that it is possible to achieve such features with a variety of different embodiments that share similar core features to the embodiments described herein.

Service Control Device Link and Continuous Heartbeat Authentication

[0318] As described herein, there are numerous ways to implement the control plane communication channel between the service processor 115 and the service controller 122. Various embodiments described herein disclose a secure and bandwidth efficient control plane that is compatible with any IP based network (including the ability to locate the service controller 122 over the Internet); provides for consistent device assisted service monitoring, control, verification and/or billing while roaming across multiple networks with different access technologies; and allows continuous device assisted service control verification and/or authentication with a variety of mechanisms for setting the transmission heartbeat frequency. Other techniques that could be used for this function include, for example, encapsulating the control plane in the access network control plane channel, encapsulating the control plane in IP

or data packet framing mechanisms (e.g., IPV6), running a more conventional VPN or IPSEC channel, and/or using an independent access network connection.

[0319] FIG. 24 is a functional diagram illustrating the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 in accordance with some embodiments. In particular, the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 as shown in FIG. 24 provide for secure control plane communication over the service control link 1653 between the service processor 115 and the service controller 122 in accordance with some embodiments. Various embodiments include two or three layers of encryption in the service control link, with one embodiment or layer being implemented in the encrypt functions (2408, 2428) and decode functions (2412, 2422), and another embodiment or layer implemented in the transport services stack (2410, 2420). An optional third embodiment or layer of encryption is implemented below the transport services stack, for example, with IPSEC or another IP layer encryption, VPN or tunneling scheme. For example, various known security encryption techniques can be implemented in the encrypt functions (2408, 2428), with public/private or completely private keys and/or signatures so that very strong levels of security for service processor control plane traffic can be achieved even through the basic transport services (2410, 2420) implemented with standard secure or open Internet networking protocols, such as TLS or TCP. For example, the service processor agent communications local to the device can be conducted to and from the service controller elements via the service control device link 1691 connection to the agent communication bus 1630. The combination of the service control device link 1691 and the agent communication bus 1630, which in some embodiments is also securely encrypted or signed, provides a seamless, highly secure, asynchronous control plane connection between the service processor and service controller server elements and the service controller and service controller agents that works over a wide range of access networks, such as any access network that has the capability to connect IP or TCP traffic to another TCP or IP endpoint on the access network, another private network or over the Internet 120. As described herein, in some embodiments, the agent communication bus 1630 also provides a fourth level of encrypted or signed communication to form a secure closed system on the device for agent to agent communication, for example, making it very difficult or practically impossible for software or applications to gain access to one or more of the a service processor agents on the device in any

way other than the service control device link 1691. In this way, in some embodiments, the agent communication bus 1630 and the service processor agents can only be accessed by one another as necessary or permitted by agent communication policies, or by the service controller or other authorized network function with proper security credentials communicating over the service control device link 1691. Additionally, in some embodiments, communications between a subset of two or more agents, or between one or more agents and one or more service controller server elements are encrypted with unique keys or signatures in such a way that a fourth level of security providing private point to point, point to multipoint, or multipoint to multipoint secure communication lines is provided.

[0320] In some embodiments, all of the service control device link 1691 communications are transformed into a continuous control plane connection, with a frequency based on the rate of service usage, a minimum set period between connections, and/or other methods for establishing communication frequency. In some embodiments, this heartbeat function provides a continuous verification link by which the service controller verifies that the service processor and/or device are operating properly with the correct service policies being implemented. In view of the following heartbeat function embodiments described herein, it will be apparent to one of ordinary skill in the art that different approaches for implementing the various heartbeat embodiments are possible, and it will be clear that there are many ways to achieve the essential features enabling a reliable, sometimes continuous control link and verification function for the purpose of assisting control of service usage in a verifiable manner. As shown, inside the service processor 115, the service control device link 1691 includes a heartbeat send counter 2402 in communication with the agent communication bus 1630. For example, the heartbeat send counter 2402 can provide a count for triggering when a service processor 115 communication (e.g., periodic communication based on a heartbeat mechanism) should be sent to the service controller 122, and a heartbeat buffer 2404, also in communication with the agent communication bus 1630, buffers any such information for the next service processor 115 communication, in accordance with various heartbeat based embodiments, as similarly described herein. The heartbeat buffer 2404 is in communication with a framing element 2406 and an encrypt element 2408 for framing and encrypting any service processor 115 communications transmitted to the service controller 122 by a transport services stack 2410 over the service control link 1653. Similarly, as shown inside the service controller 122, the service control

server link 1638 includes a heartbeat send counter 2434 in communication with a service controller network 2440, a heartbeat buffer 2432, also in communication with the service controller network 2440, buffers any such information for the next service controller 122 communication, in accordance with various heartbeat based embodiments, as similarly described herein. The heartbeat buffer 2432 is in communication with a framing element 2430 and an encrypt element 2428 for framing and encrypting any such service controller 122 communications transmitted to the service processor 115 by a transport services stack 2420 over the service control link 1653.

[0321] As also shown inside the service processor 115 of FIG. 24, the service control device link 1691 includes a decode element 2412 for decoding any received service controller 122 communications (e.g., decrypting encrypted communications), an unpack element 2414 for unpacking the received service controller 122 communications (e.g., assembling packetized communications), and an agent route 2416 for routing the received service controller 122 communications (e.g., commands, instructions, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent refreshes and/or new software for installation) to the appropriate agent of the service processor 115. Similarly, as shown inside the service controller 122, the service control server link 1638 also includes a decode element 2422 for decoding any received service processor 115 communications (e.g., decrypting encrypted communications), an unpack element 2424 for unpacking the received service processor 115 communications (e.g., assembling packetized communications), and an agent route 2426 for routing the received service processor 115 communications (e.g., responses to instructions and/or commands, heartbeat related information or status reports, policy related information or configuration settings and/or updates, challenge/response queries, agent status information, network service/cost usage and/or any other reporting related information) to the appropriate agent of the service controller 122. Accordingly, as described herein with respect to various embodiments, the various secure communications between the service controller 122 and the service processor 115 can be performed using the embodiment as shown in FIG. 24, and those of ordinary skill in the art will also appreciate that a variety of other embodiments can be used to similarly provide the various secure communications between the service controller 122 and the service processor 115 (e.g., using different software and/or hardware architectures to provide secure communications, such

as using additional and/or fewer elements/functions or other design choices for providing such secure communications).

[0322] In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided, and the following embodiments (e.g., as shown and described with respect to FIG. 25) teach such a structure that packs the various service processor agent control plane communications and the various service controller element control plane connections into a format that does not consume excessive bandwidth to enable a continuous control plane connection between the device and service controller. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to buffer such communication messages for some period of time before framing and transmitting, such as in a heartbeat frequency that is based on rate of service usage. In some embodiments, an efficient and effective communication framing structure between the service processor and service controller is provided to allow for the frame to be easily packed, encrypted, decoded, unpacked and the messages distributed. In view of the various embodiments described herein, it will be apparent to one of ordinary skill in the art that many framing structures will work for the intended purpose of organizing or framing agent communications and the uniqueness and importance of combining such a system element with the device service controller functions, the service processor functions, the service control verification functions and/or the other purposes.

[0323] FIG. 25 is a functional diagram illustrating a framing structure of a service processor communication frame 2502 and a service controller communication frame 2522 in accordance with some embodiments. In particular, the service control device link 1691 of the service processor 115 and the service control service link 1638 of the service controller 122 (e.g., as shown in FIG. 24) provide for secure control plane communication over the service control link 1653 between the service processor 115 and the service controller 122 using communication frames in the format of the service processor communication frame 2502 and the service controller communication frame 2522 as shown in FIG. 25 in accordance with some embodiments. As shown, the service processor communication frame 2502 includes a service processor framing sequence number 2504, a time stamp 2506, an agent first function ID 2508, an agent first function message length 2510, an agent first function message 2512, and assuming

more than one message is being transmitted in this frame, an agent Nth function ID 2514, an agent Nth function message length 2516, and an agent Nth function message 2518. Accordingly, the service processor communication frame 2502 can include one or more messages as shown in FIG. 25, which can depend on networking frame length requirements and/or other design choices. Similarly, as shown, the service controller communication frame 2522 includes a service controller framing sequence number 2524, a time stamp 2526, an agent first function ID 2528, an agent first function message length 2530, an agent first function message 2532, and assuming more than one message is being transmitted in this frame, an agent Nth function ID 2534, an agent Nth function message length 2536, and an agent Nth function message 2538. Accordingly, the service controller communication frame 2522 can include one or more messages as shown in FIG. 25, which can depend on networking frame length requirements and/or other design choices.

[0324] FIGS. 26A through 26H provide tables summarizing various service processor heartbeat functions and parameters (e.g., implemented by various agents, components, and/or functions implemented in software and/or hardware) in accordance with some embodiments. Many of these heartbeat functions and parameters are similarly described above, and the tables shown in FIGS. 26A-26H are not intended to be an exhaustive summary of these heartbeat functions and parameters, but rather are provided as an aid in understanding these functions and parameters in accordance with some heartbeat based embodiments described herein.

[0325] FIGS. 27A through 27P provide tables summarizing various device based service policy implementation verification techniques in accordance with some embodiments. Many of these device based service policy implementation verification techniques are similarly described above, and the tables shown in FIGS. 27A-27P are not intended to be an exhaustive summary of these device based service policy implementation verification techniques, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

[0326] FIGS. 28A through 28E provide tables summarizing various techniques for protecting the device based service policy from compromise in accordance with some embodiments. Many of these techniques for protecting the device based service policy from

compromise are similarly described above, and the tables shown in FIGS. 28A-28E are not intended to be an exhaustive summary of these techniques for protecting the device based service policy from compromise, but rather are provided as an aid in understanding these techniques in accordance with some device based service policy embodiments described herein.

Device Assisted Service Control and Traffic Control

[0327] As described below, various techniques are disclosed for implementing device assisted traffic shaping and service control at the lower levels of service usage policy implementation.

[0328] FIG. 29 is a functional diagram illustrating a device communications stack that allows for implementing verifiable traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. As shown, several service agents take part in data path operations to achieve various data path improvements, and, for example, several other service agents can manage the policy settings for the data path service, implement billing for the data path service, manage one or more modem selection and settings for access network connection, interface with the user and/or provide service policy implementation verification. Additionally, in some embodiments, several agents perform functions to assist in verifying that the service control or monitoring policies intended to be in place are properly implemented, the service control or monitoring policies are being properly adhered to, that the service processor or one or more service agents are operating properly, to prevent unintended errors in policy implementation or control, and/or to prevent tampering with the service policies or control. As shown, the service measurement points labeled I through VI represent various service measurement points for service monitor agent 1696 and/or other agents to perform various service monitoring activities. Each of these measurement points can have a useful purpose in various embodiments described herein. For example, each of the traffic measurement points that is employed in a given design can be used by a monitoring agent to track application layer traffic through the communication stack to assist policy implementation functions, such as the policy implementation agent 1690, or in some embodiments the modem firewall agent 1655 or the application interface agent 1693, in making a determination regarding the traffic parameters or type once the traffic is farther down in the communication stack where it is sometimes difficult

or impossible to make a complete determination of traffic parameters. For example, a detailed set of embodiments describing how the various measurement points can be used to help strengthen the verification of the service control implementation are described herein, including, for example, the embodiments described with respect to FIG. 16 and FIG. 21. The particular locations for the measurement points provided in these figures are intended as instructional examples, and other measurement points can be used for different embodiments, as will be apparent to one of ordinary skill in the art in view of the embodiments described herein. Generally, in some embodiments, one or more measurement points within the device can be used to assist in service control verification and/or device or service troubleshooting.

[0329] In some embodiments, the service monitor agent and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through the various communication stack formatting, processing and encryption steps, and providing the virtual tag information to the various agents that monitor, control, shape, throttle or otherwise observe, manipulate or modify the traffic. This tagging approach is referred to herein as virtual tagging, because there is not a literal data flow, traffic flow or packet tag that is attached to flows or packets, and the book-keeping to tag the packet is done through tracking or tracing the flow or packet through the stack instead. In some embodiments, the application interface and/or other agents identify a traffic flow, associate it with a service usage activity and cause a literal tag to be attached to the traffic or packets associated with the activity. This tagging approach is referred to herein as literal tagging. There are various advantages with both the virtual tagging and the literal tagging approaches. For example, it can be preferable in some embodiments to reduce the inter-agent communication required to track or trace a packet through the stack processing by assigning a literal tag so that each flow or packet has its own activity association embedded in the data. As another example, it can be preferable in some embodiments to re-use portions of standard communication stack software or components, enhancing the verifiable traffic control or service control capabilities of the standard stack by inserting additional processing steps associated with the various service agents and monitoring points rather than re-writing the entire stack to correctly process literal tagging information, and in such cases, a virtual tagging scheme may be desired. As yet another example, some standard communication stacks provide for unused, unspecified or otherwise available bit fields in a packet frame or flow, and these unused, unspecified or otherwise available bit fields can be used to literally tag traffic without the need to

re-write all of the standard communication stack software, with only the portions of the stack that are added to enhance the verifiable traffic control or service control capabilities of the standard stack needing to decode and use the literal tagging information encapsulated in the available bit fields. In the case of literal tagging, in some embodiments, the tags are removed prior to passing the packets or flows to the network or to the applications utilizing the stack. In some embodiments, the manner in which the virtual or literal tagging is implemented can be developed into a communication standard specification so that various device or service product developers can independently develop the communication stack and/or service processor hardware and/or software in a manner that is compatible with the service controller specifications and the products of other device or service product developers.

[0330] It will be appreciated that although the implementation/use of any or all of the measurement points illustrated in FIG. 29 is not required to have an effective implementation, such as was similarly shown with respect to various embodiments described herein, such as with respect to FIGS. 19 and 21, various embodiments can benefit from these and/or similar measurement points. It will also be appreciated that the exact measurement points can be moved to different locations in the traffic processing stack, just as the various embodiments described herein can have the agents affecting policy implementation moved to different points in the traffic processing stack while still maintaining effective operation. In some embodiments, one or more measurement points are provided deeper in the modem stack (e.g., such as for embodiments similarly described herein with respect to FIGS. 35 and 36) where, for example, it is more difficult to circumvent and can be more difficult to access for tampering purposes if the modem is designed with the proper software and/or hardware security to protect the integrity of the modem stack and measurement point(s).

[0331] Referring to FIG. 29, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Example measurement point VI resides within or just above the modem driver layer. For example, the modem driver performs modem bus communications, data protocol translations, modem control and configuration to interface the networking stack traffic to the modem. As shown, measurement point VI is common to all modem drivers and modems,

and it is advantageous for certain embodiments to differentiate the traffic or service activity taking place through one modem from that of one or more of the other modems. In some embodiments, measurement point VI, or another measurement point, is located over, within or below one or more of the individual modem drivers. The respective modem buses for each modem reside between example measurement points V and VI. In the next higher layer, a modem selection & control layer for multimode device based communication is provided. In some embodiments, this layer is controlled by a network decision policy that selects the most desirable network modem for some or all of the data traffic, and when the most desirable network is not available the policy reverts to the next most desirable network until a connection is established provided that one of the networks is available. In some embodiments, certain network traffic, such as verification, control, redundant or secure traffic, is routed to one of the networks even when some or all of the data traffic is routed to another network. This dual routing capability provides for a variety of enhanced security, enhanced reliability or enhanced manageability devices, services or applications. In the next higher layer, a modem firewall is provided. For example, the modem firewall provides for traditional firewall functions, but unlike traditional firewalls, in order to rely on the firewall for verifiable service usage control, such as access control and security protection from unwanted networking traffic or applications, the various service verification techniques and agents described herein are added to the firewall function to verify compliance with service policy and prevent tampering of the service controls. In some embodiments, the modem firewall is implemented farther up the stack, possibly in combination with other layers as indicated in other figures. In some embodiments, a dedicated firewall function or layer is provided that is independent of the other processing layers, such as the policy implementation layer, the packet forwarding layer and/or the application layer. In some embodiments, the modem firewall is implemented farther down the stack, such as within the modem drivers, below the modem drivers, or in the modem itself. Example measurement point IV resides between the modem firewall layer and an IP queuing and routing layer. As shown, an IP queuing and routing layer is separate from the policy implementation layer where the policy implementation agent implements a portion of the traffic control and/or service usage control policies. As described herein, in some embodiments, these functions are separated so that a standard network stack function can be used for IP queuing and routing, and the modifications necessary to implement the policy implementation agent functions can be provided

in a new layer inserted into the standard stack. In some embodiments, the IP queuing and routing layer is combined with the traffic or service usage control layer. Examples of this combined functionality are shown and described with respect to FIGS. 31, 32 and 33. For example, a combined routing and policy implementation layer embodiment can also be used with the other embodiments, such as shown in FIG. 29. Various detailed embodiments describing how the policy implementation layer can control traffic or other service usage activities are described with respect to FIG. 38. Measurement point III resides between the IP queuing and routing layer and a policy implementation agent layer. Measurement point II resides between the policy implementation agent layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 29.

[0332] As shown, the application service interface layer is above the standard networking stack API and, in some embodiments, its function is to monitor and in some cases intercept and process the traffic between the applications and the standard networking stack API. In some embodiments, the application service interface layer identifies application traffic flows before the application traffic flows are more difficult or practically impossible to identify farther down in the stack. In some embodiments, the application service interface layer in this way assists application layer tagging in both the virtual and literal tagging cases. In the case of upstream traffic, the application layer tagging is straight forward, because the traffic originates at the application layer. In some downstream embodiments, where the traffic or service activity classification relies on traffic attributes that are readily obtainable, such as source address or URL, application socket address, IP destination address, time of day or any other readily obtained parameter, the traffic type can be identified and tagged for processing by the firewall agent or another agent as it initially arrives. In other embodiments, as described herein, in the downstream case, the solution is generally more sophisticated when a traffic parameter that is needed to classify the manner in which the traffic flow is to be controlled or throttled is not readily available at the lower levels of the stack, such as association with an aspect of an

application, type of content, something contained within TLS, IPSEC or other secure format, or other information associated with the traffic. Accordingly, in some embodiments the networking stack identifies the traffic flow before it is fully characterized, categorized or associated with a service activity, and then passes the traffic through to the application interface layer where the final classification is completed. In such embodiments, the application interface layer then communicates the traffic flow ID with the proper classification so that after an initial short traffic burst or time period the policy implementation agents can properly control the traffic. In some embodiments, there is also a policy for tagging and setting service control policies for traffic that cannot be fully identified with all sources of tagging including application layer tagging.

[0333] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630, communicates user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or configuration information via this communications bus 1630, as shown (illustrating such communications with a reference (B) via the application layer, policy implementation agent layer, which is lower in the communications stack as shown, and/or the modem firewall layer). The connection manager agent communicates select and control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C) via the modem selection and control layer). Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (D) at the application layer, (E) at the policy implementation agent layer, and (F) at the modem firewall layer).

[0334] As shown in FIG. 29, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through VI, receiving information including application information, service usage and other service related information, and assignment information. An access

control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown.

[0335] In some embodiments, one or more of the networking stack modifications described herein in combination one or more of the service verification and tamper prevention techniques described herein is provided. As similarly described with respect to FIG. 29, the various example embodiments for assisting service control verification described herein and as summarized in the example tables provided in FIGS. 26, 27 and 28 can be employed individually or in combination to create increasingly secure cross-functional service control verification embodiments. In FIG. 29, the presence of the access control integrity agent, policy control agent, service monitor agent and the other agents that perform verification and/or tamper prevention functions illustrates verifiable service control aspects in accordance with some embodiments. Furthermore, the presence of the billing agent combined with the service verification and/or tamper prevention agents and techniques described herein provides for a set of verifiable billing embodiments for service billing, service billing offset corrections, bill by account, transaction billing and other billing functions. In addition, the presence of the user service interface agent in combination with the service control agent functions in the modified networking stack provide for embodiments involving a combination of service control with user preferences, which as described herein, provides the user with the capability to optimize service versus service cost in a network neutral manner. In some embodiments, the user control of service control policy is provided along with the service control verification and/or tamper prevention. The presence of the policy control agent that in some embodiments implements a higher than most basic level of policy decision and control with the policy implementation agents in the modified networking stack allows for, for example, the device to possess the capability to implement a higher level of service control for the purpose of obtaining a higher level service usage or service activity objective. In some embodiments, the application layer tagging in combination with other embodiments described herein provides for deep service activity control that is verifiable.

[0336] In some embodiments, verifiable traffic shaping as described herein can be performed using the device communications stack in a variety of embodiments for the combination of service control within the networking stack and service control verification

and/or tamper prevention, with various embodiments depicted in FIGS. 29 through 37. Additional levels of detail regarding how such embodiments can be used to implement verifiable traffic shaping are provided in and described with respect to FIGS. 38 through 40 which depict example functional diagrams of packet processing flows for verifiable traffic shaping or service activity control in a device service processor for both upstream and downstream flows. Along with several other interesting features embodied in FIGS. 38 through 40, application traffic layer tagging is depicted in additional detail in accordance with some embodiments. For example, the application interface agent can determine service data usage at the application layer using measurement point I and a local service usage counter, and can, for example, pass this information to the service monitor agent. If service usage exceeds a threshold, or if using a service usage prediction algorithm results in predicted service usage that will exceed a threshold, then the user can be notified of which applications are causing the service usage overrun or potential service usage overrun, via the user service interface agent. The user can then identify which application service (e.g., traffic associated with a specified high service use or non-critical application, such as for example a high bandwidth consumption social networking website or service, media streaming website or service, or any other high bandwidth website or service transmitting and/or receiving data with the service network) that the user prefers to throttle. As another example, the user could select a service policy that allows for video chat services until those services threaten to cause cost over-runs on the user's service plan, and at that time the service policy could switch the chat service to voice only and not transmit or receive the video. The traffic associated with the user specified application can then be throttled according to user preference input. For example, for downstream traffic, packets (e.g., packets that are virtually or literally tagged and/or otherwise associated with the application traffic to be throttled) from the access network can be buffered, delayed and/or dropped to throttle the identified application traffic. For upstream traffic, packets (e.g., packets that are virtually or literally tagged and/or otherwise associated with the application traffic to be throttled) can be buffered, delayed and/or dropped before being transmitted to the access network to throttle the identified application traffic. As similarly described above, traffic shaping as described herein can be verified, such as by the service monitor agent via the various measurement points and/or using other agents.

[0337] The embodiments depicted in FIG. 30 and other figures generally require enhancements to conventional device networking communication stack processing. For

example, these enhancements can be implemented in whole or in part in the kernel space for the device OS, in whole or in part in the application space for the device, or partially in kernel space and partially in application space. As described herein, the networking stack enhancements and the other elements of the service processor can be packaged into a set of software that is pre-tested or documented to enable device manufacturers to quickly implement and bring to market the service processor functionality in a manner that is compatible with the service controller and the applicable access network(s). For example, the service processor software can also be specified in an interoperability standard so that various manufacturers and software developers can develop service processor implementations or enhancements, or service controller implementations or enhancements that are compatible with one another.

[0338] FIG. 30 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, a portion of the service processor is implemented on the modem (e.g., on modem module hardware or modem chipset) and a portion of the service processor is implemented on the device application processor subsystem. It will be apparent to one of ordinary skill in the art that variations of the embodiment depicted in FIG. 30 are possible where more or less of the service processor functionality is moved onto the modem subsystem or onto the device application processor subsystem. For example, such embodiments similar to that depicted in FIG. 30 can be motivated by the advantages of containing some or all of the service processor network communication stack processing and/or some or all of the other service agent functions on the modem subsystem (e.g., and such an approach can be applied to one or more modems). For example, the service processor can be distributed as a standard feature set contained in a modem chipset hardware or software package or modem module hardware or software package, and such a configuration can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity or security, specification or interoperability standardization, and/or other benefits.

[0339] Referring to FIG. 30, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a

communication layer for modem MAC/PHY layer at the bottom of the device communications stack. Measurement point IV resides above the modem MAC/PHY layer. The modem firewall layer resides between measurement points IV and III. In the next higher layer, the policy implementation agent is provided, in which the policy implementation agent is implemented on the modem (e.g., on modem hardware). Measurement point II resides between the policy implementation agent and the modem driver layer, which is then shown below a modem bus layer. The next higher layer is shown as the IP queuing and routing layer, followed by the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 30.

[0340] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communicates user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent B communicates service settings and/or configuration information via this communications stack, as shown (illustrating such communications with a reference (B)) via the application layer. The policy control agent A communicates service settings and/or configuration information via this communications stack, as shown (illustrating such communications with a reference (D)) via the policy implementation agent layer and/or the modem firewall layer. The connection manager agent communicates select & control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C)) via the modem driver layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (E)) at the application layer through the modem driver layer with the service monitor agent B as shown (and an access control integrity agent B is also shown), and communications with references (F) at the policy implementation

agent layer and (G) at the modem firewall layer with the service monitor agent A as shown (and an access control integrity agent A is also shown). In some embodiments, the service usage policy verification or tamper prevention embodiments described herein can be applied, in isolation or in combination, in the context of FIG. 31 to provide for embodiments with increasing levels of service usage policy control verification certainty, such as provided with FIGS. 26A-26H, 27A-27P and 28A-28E.

[0341] FIG. 31 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the service processor is a simplified implementation. For example, this approach can be used for applications with less capable device application processors, rapid time to market needs, fewer service usage control needs, and/or other reasons that lead to a need for a lower complexity implementation.

[0342] Referring to FIG. 31, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for the modem layer at the bottom of the device communications stack. The modem driver layer resides above the modem bus layer as shown. In the next higher layer, the policy implementation agent is provided, and the policy implementation agent is also in communication with the agent communication bus 1630 as shown. The next higher layer is shown as the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown. The connection manager communicates select and control as well as modem and access network information via the modem driver as shown. Although FIG. 31 does not depict all of the service usage control verification functions provided by certain embodiments calling for additional service verification or control agents, a high level of service policy implementation verification certainty can be

achieved within the context of the embodiments depicted in FIG. 31 by applying a subset of the service usage policy verification or tamper prevention embodiments described herein. For example, the embodiments depicted in FIG. 31 can be combined with the service controller embodiments that utilize IPDRs to verify service usage is in accordance with the desired service policy. There are also many other service usage control embodiments described herein that can be applied in isolation or in combination to the embodiments depicted in FIG. 31 to provide increasing levels of service usage control verification certainty, as will be apparent to one of ordinary skill in the art in view of FIGS. 26A-26H, 27A-27P and 28A-28E and the various embodiments described herein.

[0343] FIG. 32 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the service processor is a simplified implementation embodiment with device based monitoring and integrity control. For example, FIG. 32 provides for somewhat higher complexity (e.g., relative to the embodiments depicted in FIG. 30) in exchange for the enhanced service monitoring, control or verification that are possible by implement additional agent embodiments, such as the service monitor agent and the access control integrity agent functions.

[0344] Referring to FIG. 32, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point II resides above the modem selection & control layer, which resides above the modem buses for each modem. Measurement point I resides between the policy implementation agent (policy based router/firewall) layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown. The connection manager communicates select and

control as well as modem and access network information via the modem selection and control layer as shown. The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. As similarly described with respect to FIGS. 30 and 31, many of the service usage control verification embodiments described herein can be applied in isolation or in combination in the context of FIG. 32.

[0345] FIG. 33 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. Referring to FIG. 33, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point III resides above the modem selection & control layer, which resides above the respective modem buses for each modem. Measurement point II resides between the policy implementation agent (policy based router/firewall) layer and the transport layer, including TCP, UDP, and other IP as shown. The session layer resides above the transport layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer. Measurement point I resides between the network services API layer and an application layer, shown as application service interface agent in the device communications stack of FIG. 33.

[0346] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communicates user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or

configuration information via this communications stack, as shown (illustrating such communications with a reference (B)) via the policy implementation agent layer. The connection manager agent communicates select & control commands and/or modem and access network information via this communications stack, as shown (illustrating such communications with a reference (C)) via the modem selection and control layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (D)) at the application layer and (E) at the policy implementation agent layer.

[0347] As shown in FIG. 33, a service monitor agent, which is also in communication with the agent communication bus 1630, communicates with various layers of the device communications stack. For example, the service monitor agent, performs monitoring at each of measurement points I through III, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. As similarly described with respect to FIGS. 30, 31 and 32, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 33.

[0348] FIG. 34 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In some embodiments, the data path processing for the service processor is provided in conjunction with a single modem driver as shown. As shown, the service processor communication stack processing is provided below the standard network communication stack and in combination with a modem driver (e.g., and this approach can be extended to more than one modem).

[0349] Referring to FIG. 34, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. Measurement point II resides above the modem driver 1 layer.

Measurement point I resides between the policy implementation agent (policy based router/firewall) layer and the modem selection and control layer, for the modem driver 1 stack in this single modem driver embodiment. The transport layer, including TCP, UDP, and other IP resides above the IP queuing and routing layer, which resides above the modem selection and control layer, as shown. The session layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer, resides above the transport layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer.

[0350] As shown in FIG. 34, applications communicate with the device communications stack via the network services API as shown (illustrating such communications with a reference (A)). Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown (illustrating such communications with a reference (B)). The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with policy implementation agent layer of the device communications stack. Also, the service monitor agent performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information. An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information, application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (C)) at the policy implementation agent layer. Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. As similarly described with respect to FIGS. 30, 31, 32 and 33, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 34.

[0351] FIG. 35 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 35 illustrates a

single modem hardware embodiment as shown. As shown, the service processor network communication stack processing is provided on the modem hardware (e.g., and this approach can be extended to more than one modem). This approach allows for the service processor to be distributed as a standard feature set contained in a modem chipset hardware or software package or modem module hardware or software package, which, for example, can provide for easier adoption or development by device OEMs, a higher level of differentiation for the chipset or modem module manufacturer, higher levels of performance or service usage control implementation integrity, or other benefits.

[0352] Referring to FIG. 35, describing the device communications stack from the bottom to the top of the stack as shown, the device communications stack provides a communication layer for each of the modems of the device at the bottom of the device communications stack. As shown, measurement points I and II and the policy implementation agent reside on the modem 1 (e.g., implemented as hardware and/or software on modem 1). Measurement point I resides above the policy implementation agent (policy based router/firewall) layer, and measurement point II resides below the policy implementation agent layer. The modem selection and control layer resides above the modem drivers layer, as shown. The transport layer, including TCP, UDP, and other IP resides above the IP queuing and routing layer, which resides above the modem selection and control layer, as shown. The session layer, which is shown as a socket assignment and session management (e.g., basic TCP setup, TLS/SSL) layer, resides above the transport layer. The network services API (e.g., HTTP, HTTPS, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3, DNS) resides above the session layer.

[0353] As shown in FIG. 35, applications communicate with the device communications stack via the network services API as shown. Policy settings from the network (e.g., service settings) are communicated with the policy implementation agent as shown (illustrating such communications with a reference (A)). The service monitor agent, which is also in communication with the agent communication bus 1630, communicates with policy implementation agent layer of the modem 1. Also, the service monitor agent performs monitoring at each of measurement points I and II, receiving information including application information, service usage and other service related information, and assignment information.

An access control integrity agent is in communication with the service monitor agent via the agent communications bus 1630, as also shown. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with references (B)) at the policy implementation agent layer. As similarly described with respect to FIGS. 30, 31, 32, 33 and 34, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 35.

[0354] FIG. 36 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 36 illustrates a single modem hardware embodiment, in which modem 1 includes a portion of the service processor networking communication stack processing and measurement points II and III and the policy implementation agent, as similarly shown in FIG. 35, and the higher levels of the device communications stack above the modem 1 layer, such as the application service interface layer, are implemented on the device application processor or in the device application processor memory as similarly described above, for example, with respect to FIG. 33, in which a measurement point I is shown between the application service interface agent layer and the network services API layer. For example, this approach allows for the application service interface agent to be provided on the device application processor or memory so that application layer service usage monitoring or control can be implemented. For example, the differences between the embodiments depicted in FIG. 36 and those of FIG. 30 include a simplified implementation and a policy control agent that is entirely implemented on the modem and not partially implemented in the application processor memory.

[0355] Various applications and/or a user service interface agent communicate via this communications stack, as shown (illustrating such communications with a reference (A)). Also, the billing agent, which is in communication with the agent communication bus 1630 communications user information and decision query and/or user input to the user service interface agent, as shown. The policy control agent communicates service settings and/or configuration information via this communications stack, as shown (illustrating such

communications with a reference (B)) via the policy implementation agent layer. Various other communications (e.g., service processor and/or service controller related communications, such as service usage measure information and/or application information) are provided at various levels of this communications stack, as shown (illustrating such communications with reference (C) at the application layer and communications with reference (D) at the policy implementation agent layer). As shown, the service monitor agent B communicates with the application service interface agent and measurement point I, and the service monitor agent A communicates with the policy implementation agent layer and measurement points II and III of the modem 1. As similarly described with respect to FIGS. 30, 31, 32, 33, 34 and 35, many of the service usage control verification embodiments disclosed herein can be applied in isolation or in combination in the context of FIG. 36.

[0356] FIG. 37 is another functional diagram illustrating the device communications stack that allows for implementing traffic shaping policy, access control policy and/or service monitoring policy in accordance with some embodiments. In particular, FIG. 37 illustrates a device communications stack as similarly shown in FIG. 36, with the difference being that the service processor subsystem networking communication stack processing is implemented on a hardware function that is separate from the application processor and the modem. For example, this approach provides security advantages with a dedicated hardware system to protect some or all of the service usage control system from tampering. For example, some or all of the service processor can be implemented on a SIM card module. As another example, some or all of the service processor can be encapsulated on a self contained hardware module that can be added to a device without the need to modify the networking communication stack software or hardware.

[0357] FIG. 38 is a functional diagram illustrating a device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG. 38. For example, the service processor packet processing flow can be performed by the device communications stack, such as described above with respect to FIG. 29. The various embodiments for packet processing flow depicted in FIGS. 38 through 40 are self explanatory to

one of ordinary skill in the art and not all the processing steps and flow sequences are described herein.

[0358] In some embodiments, the burst size, buffer delay, acknowledgement delay and drop rate used in upstream and downstream traffic shaping are optimized with the goal of reducing access network traffic overhead, and excess capacity usage that can result from mismatches in traffic transmission parameters with the access network MAC and PHY or from excess network level packet delivery protocol re-transmissions. In some embodiments, an application interface agent 1693 is used to literally tag or virtually tag application layer traffic so that the policy implementation agent(s) 1690 has the necessary information to implement selected traffic shaping solutions. As shown in FIG. 16, the application interface agent 1693 is in communication with various applications, including a TCP application 1604, an IP application 1605, and a voice application 1602.

[0359] Referring to FIGS. 38 through 40, in some embodiments, the upstream traffic service policy implementation step corresponds to the traffic shaping step described herein. Referring to FIG. 38, this step is depicted as shown as an alternate exploded view including four upstream sub-steps of apply QoS queue priority, apply traffic shaping rules, network optimized buffer/delay and remove application ID tag. An additional approach shown in FIG. 38 involves two exploded view sub-steps associated with the firewall service policy implementation step and these sub-steps are pass/block packet and pass/redirect packet. For example, the functions performed by these six sub-steps can be depicted in any number of sub-steps, the order of the steps can be appropriately performed in various different orders to provide for upstream traffic shaping within the network communication stack. For example, FIGS. 39 and 40 show the two steps of policy implementation and firewall as one step and the six exploded view sub-steps are included under the same policy implementation step and are performed in a different order than in FIG. 38. It should also be noted that a number of embodiments are possible in which the access control, traffic control or firewall functions are moved to the application service interface layer or another layer.

[0360] Referring now to the downstream portion of FIG. 38, there are two steps again termed traffic service policy implementation and firewall service policy implementation in this

traffic shaping, access control and firewall example. These two packet flow processing steps are depicted as shown in the exploded view as the five sub-steps of tag with flow ID, pass/block packet, apply QoS, apply traffic shaping rules and network optimized buffer, delay, and drop. As with the upstream packet processing flow, the number of sub-steps, the order of sub-steps and the location of the sub-steps in the downstream networking stack processing can be depicted in any number of sub-steps, order and/or location, and various other embodiments will be apparent to one of ordinary skill in the art, including embodiments which locate some or all of the steps in the application service interface layer or other layers as depicted in FIGS. 39 and 40. The details of the packet flow processing design for the downstream can be somewhat more complex in certain embodiments as compared to the upstream processing in two ways. First, as described herein, in some embodiments, the packet tagging that requires application level information can require the initial portion of the packet flow burst to pass through the upstream networking communication stack until the application service interface layer can associate the packet flow with the appropriate information visible at the application level at which time the packet flow tag is communicated to the other service processor agent functions so that they can properly monitor or control the traffic associated with the flow.

[0361] Independently, another complication arises when upper layer reliable communication protocols, such as TCP, are employed in the networking stack in which the downstream transmitting end repeats the packet transmission if the receiving TCP protocol stack does not send a packet receipt acknowledge (ACK) within a certain period of time. If packets are arbitrarily delayed or dropped, then the TCP re-transmission traffic can reduce, completely eliminate or even reverse the network capacity advantage gained by reducing the average traffic speed or other transmission quality measure for one or more service activities. To solve this problem, in some embodiments, the packet traffic control parameters (e.g., downstream delay, drops, burst length, burst frequency and/or burst jitter) are optimized for TCP re-transmission efficiency so that changes in traffic control access bandwidth or speed for one or more service activities are implemented in such a manner that the TCP re-transmission delay at the network transmitting end adapts to be long enough so that wasted packet re-transmission bandwidth is reduced. In addition, and either in combination or in isolation, in some embodiments, the packet traffic control parameters (e.g., downstream delay, drops, burst length, burst frequency and/or

burst jitter) can be adjusted so that the access network downstream MAC and/or PHY efficiencies are optimized.

[0362] Numerous other embodiments for the detailed implementation of packet flow processing in both downstream and upstream will be apparent to one of ordinary skill in the art in view of the various embodiments described herein. In some embodiments, as described herein, the following are provided: (A) traffic shaping is performed in a verifiable manner, (B) traffic shaping is performed in a manner that results in improved network capacity by taking into account to some degree the manner in which the access network PHY layer and/or MAC layer responds to packet parameters (e.g. burst delay, burst drops, burst length, burst frequency and/or burst jitter), (C) traffic shaping is performed in a manner that results in improved network capacity by taking into account how the packet parameters (e.g., burst delay, burst drops, burst length, burst frequency and/or burst jitter) impact layer 3 and higher ACK protocol or other network protocol network capacity efficiencies, (D) packet shaping is performed in a manner that is aware of and optimized for the particular type of communication protocol or packets being sent (e.g., TCP packets can be dropped to slow the application rate of transfer whereas UDP packets are never dropped, because there is no re-transmission), (E) a virtual or literal packet tagging system is used in a verifiable traffic shaping service control system to provide a deeper level of service monitoring and control or to simplify the processing of the packets, and/or (F) starting with these low level packet processing, traffic control or access control building blocks one or more additional layers of higher level policy control can be added on the device or in the network to create service profiles for the service provider network that define complete services, such as ambient services and many other variations of service profile settings that each define a device or user service experience and can be associated with a billing plan. For example, the use of higher layers of service profile control to form more complete service solutions starting with these relatively simple low-level traffic control, access control or firewall processing steps or functions is also described herein.

[0363] FIG. 39 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG.

39 (e.g., of a less feature rich device service processor embodiment, such as one similar to that depicted in FIG. 32).

[0364] FIG. 40 is another functional diagram illustrating the device service processor packet processing flow in accordance with some embodiments. In particular, both an example upstream service processor packet processing flow (device to the network) and an example downstream service processor packet processing flow (network to the device) are shown in FIG. 40 (e.g., of a mid-featured embodiment of a device service processor, such as one similar to that depicted in FIG. 33).

[0365] FIG. 41 provides a table summarizing various privacy levels for service history reporting in accordance with some embodiments. Many of these privacy levels are similarly described above, and the table shown in FIG. 41 is not intended to be an exhaustive summary of these privacy levels, but rather is provided as an aid in understanding these privacy levels in accordance with user privacy related embodiments described herein. For example, there are many other parameters that can be associated with privacy filtering, and as will be apparent to one of ordinary skill in the art in view of the various embodiments described herein, the unique feature of user defined or user influenced privacy filtering for service usage, service activity or CRM reports can be implemented with a variety of embodiments that are variations of those described herein.

[0366] FIGS. 42A through 42J provide tables summarizing various service policy control commands in accordance with some embodiments. Many of these service policy control commands are similarly described above, and the tables shown in FIGS. 42A-J are not intended to be an exhaustive summary of these service policy control commands and do not include summaries of all the embodiments described herein, but rather are provided as a summary aid in understanding these service policy control commands in accordance with various embodiments described herein.

[0367] In some embodiments, QoS is employed for devices with a service processor 115. For example, QoS can be employed in a crowded hot spot where the service processor 115 profile has been changed from WWAN to WLAN, but the WLAN is backed up as too many users are trying to use it. The service processor 115 can have a hierarchical access to the hotspot

at that point; or the service processor 115 that pays less can be throttled while those that pay more are opened up; or the service processor 115 can initiate a policy that slows down transmissions to improve trunking efficiency.

[0368] FIGS. 43A through 43B are flow diagrams illustrating a flow diagram for a service processor authorization sequence as shown in FIG. 43A and a flow diagram for a service controller authorization sequence as shown in FIG. 43B in accordance with some embodiments.

[0369] Referring to FIG. 43A, at 4302, the device is in an offline state. At 4304, the service processor (e.g., service processor 115) of the device collects device service processor credentials and access control integrity information. At 4306, the service processor of the device selects a best network. At 4308, the device connects to an access network. At 4310, the service processor of the device sends an authorization request to the service controller (e.g., service controller 122) and also sends the credentials and access control integrity information. At 4312, the service processor determines whether an integrity error has occurred. If so, then the service processor performs integrity error handling at 4314. Otherwise, the service processor determines whether the device is activated and/or authorized for network access at 4316. If not, then the service processor performs a device activation sequence at 4318. At 4320, the service processor performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4322, the device is in an online state.

[0370] Referring to FIG. 43B, at 4332, device control is in an offline state. At 4334, the service controller (e.g., service controller 122) receives a device authorization request, verifies device service plan standing, verifies device access control integrity standing, verifies device access control integrity information, verifies service processor heartbeat, and performs various additional service processor integrity checks (e.g., as similarly described herein). At 4336, the service controller determines whether the device integrity checks have all passed. If not, then the service controller sends an integrity error to the service processor (e.g., service processor 115) at 4338. At 4340, the service controller performs integrity error handling. Otherwise (the device integrity checks have all passed), the service controller determines whether the device is

activated at 4342. If not, then the service controller sends an activation message to the service processor at 4344. At 4346, the service controller performs a service activation sequence. Otherwise (the device is activated), the service controller sends an authorization at 4348. At 4350, the service controller performs the following: updates critical software on the service processor, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, sends stored CRM and billing information. At 4352, the service controller is in a device online state.

[0371] FIGS. 44A through 44B are flow diagrams illustrating a flow diagram for a service processor activation sequence as shown in FIG. 44A and a flow diagram for a service controller activation sequence as shown in FIG. 44B in accordance with some embodiments.

[0372] Referring to FIG. 44A, at 4402, a service processor activation sequence is initiated. At 4404, the service processor (e.g., service processor 115) of the device displays an activation site (e.g., HTTP site, WAP site or portal) to the user for the user's service activation choice. At 4406, the user selects service plan, billing information and CRM information. At 4408, the service processor sends an activation request and user billing and CRM information to, for example, the service controller. At 4410, the service processor determines whether there is an integrity error. If so, then the service processor performs integrity error handling at 4412. Otherwise, the service processor determines whether there has been a selection input error at 4414. If so, the service processor displays the selection input error to the user at 4416 and returns to the activation site/portal at 4404. Otherwise, the service processor identifies the activated service plan at 4418. At 4420, the service processor performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4422, the device is in an online and activated state.

[0373] Referring to FIG. 44B, at 4432, a service controller activation sequence is initiated. At 4434, the service controller (e.g., service controller 122) receives an activation request, including user billing and CRM information, and sends such to central billing. At 4436,

the service controller receives a response from central billing. At 4438, the service controller verifies the integrity of the service processor. If an integrity error is detected, then an integrity error is sent at 4440. At 4442, the service controller performs integrity error handling. At 4444, the service controller determines whether the service plan has been activated. If not, then the service controller sends a selection input error to the device at 4446 and returns to 4432. Otherwise (device has been activated), the service controller sends the service plan activation information to the device at 4448. At 4450, the service controller performs the following: updates critical software, initializes service policy and control settings, synchronizes service counters, updates service cost data, applies policy settings, applies CRM rules settings, obtains transaction identity certificate, and sends stored CRM and billing information. At 4452, the service controller is in a device online and activated state.

[0374] FIGS. 45A through 45B are flow diagrams illustrating a flow diagram for a service processor access control sequence as shown in FIG. 45A and a flow diagram for a service controller access control sequence as shown in FIG. 45B in accordance with some embodiments.

[0375] Referring to FIG. 45A, at 4502, the device is in an online state. At 4504, the service processor (e.g., service processor 115) of the device processes any new heartbeat messages received from the service controller (e.g., service controller 122). At 4506, the service processor updates software if necessary, updates service policy and control settings if necessary, synchronizes service counters, updates service cost data if necessary, and updates CRM rules if necessary. At 4508, the service processor performs access control integrity checks. At 4510, the service processor determines whether there are any access control integrity errors. If so, then the service processor performs integrity error handling at 4512. Otherwise, the service processor updates user service UI gauges, provides notification if necessary, and accepts input if available at 4514. At 4516, the service processor sends new service processor heartbeat messages to the heartbeat message queue. At 4518, the service processor processes any pending billing transactions. At 4520, the service processor determines if a heartbeat transmission is due, and if not, returns to 4504 for processing any received heartbeat messages. If so, at 4522, the service processor sends the new service processor heartbeat message to the service controller.

[0376] Referring to FIG. 45B, at 4532, the device is in an online state. At 4534, the service controller (e.g., service controller 122) processes any new heartbeat messages received from the service processor. At 4536, the service controller performs access control integrity checks. At 4538, the service controller determines whether there are any access control integrity errors. If so, then the service controller performs integrity error handling at 4540. At 4542, the service controller updates the billing database, updates the CRM information, synchronizes service counters, updates cost database if needed, and synchronizes CRM rules if necessary. At 4544, the service controller processes any pending billing transactions. At 4546, the service controller sends new service processor heartbeat messages to the heartbeat message queue. At 4548, the service controller determines if a heartbeat transmission is due, and if not, returns to 4534 for processing any received heartbeat messages. If so, at 4550, the service controller sends new service processor heartbeat message to the service processor.

Open Content Distribution and Transaction System

[0377] Referring now to FIGS. 46 and 47A-47B, in another set of embodiments an open, decentralized, device based system for enabling central billing for third party electronic commerce transactions for mobile commerce is provided as shown. For example, in these embodiments, device information can be embedded in HTTP, WAP or other portal browser/network header request information that indicates a central billing option is available to a compatible third party transaction server, as further described below with respect to FIGS. 46 and 47A-47B.

[0378] FIG. 46 is a functional diagram illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments. As shown, a service processor 4615 of the device 100 (e.g., any mobile device capable of storing and executing the service processor 4615) includes access control integrity agent 1694, billing agent 1695, agent communication bus 1630, user interface 1697, policy control agent 1692, service monitor agent 1696, application interface agent 1693, policy implementation agent 1690, and modem router and firewall 1655, as similarly described herein with respect to various other service processor embodiments. In some embodiments, an application 4604 (e.g., an HTML/WAP web browser) and a mobile payment agent 4699 are also included in the device, such as part of the service

processor 4615 as shown. In some embodiments, the application 4604 is not integrated as part of the service processor 4615, but is executing and/or stored on the device. In some embodiments, the mobile payment agent 4699 includes billing agent 1695, user interface 1697 and/or application interface agent 1693, and/or various other functional components/agents. As shown, the service processor 4615 is in communication with a carrier access network 4610, which is in network communication with the Internet 120.

[0379] In some embodiments, device information can be embedded in HTTP, WAP or other portal browser/network header request information that indicates a central billing option is available to a compatible third party transaction server, such as the open content transaction partner site(s) 134. For example, the compatible transaction server can then send a signed confirmation request over a pre-assigned control socket channel to the billing agent 1695 with the billing agent 1695 confirming the signed confirmation request by either performing the signature check locally based on a stored and synchronized list of approved transaction servers or by passing the signed request onto a billing server 4630 for confirmation. Optionally, in another example, a triangle confirmation can be set up in which the billing server 4630 can confirm the transaction set up with the transaction server 134 or the transaction server 134 can confirm the transaction set up with the billing server 4630. Once the device confirms the compatible and approved status of the transaction server 134, the device/transaction server pair can then optionally further exchange keys for the remainder of the transaction for enhanced security. In another example, the transaction server 134 can also redirect the user browsing experience to one tailored to one or more of device type, service provider, device manufacturer or user. When the user selects a transaction, the transaction server sends the billing agent 1695 a transaction bill that describes the transaction and the amount. The billing agent 1695 can optionally confirm that the user account has sufficient credit limit to make the purchase by either confirming the stored credit limit on the device or querying the billing server 4630. The billing agent 1695 then invokes the device UI 1697 to display the transaction description and amount and request user approval for the billing to be conducted through the central billing option. User approval can be acquired, for example, by a simple click operation or require a secure password, key and/or biometric response from the user. Upon user approval, the billing agent 1695 generates a billing approval and sends it to the transaction server 134, the transaction server 134 completes the transaction and then sends a bill to the billing agent 1695. The billing agent 1695 optionally

sends a confirmation to the transaction server 134 and sends the bill to the billing server 4630. Again, optionally a triangle confirmation can be formed by the billing server sending a confirmation to the transaction server 134, or the transaction server 134 can send the bill to the billing server 4630. In some embodiments, the billing server 4630 can also communicate such billed transactions to a central provider billing system 4623 via the carrier access network 4610. Also, in some embodiments, an alternate location billing server 4632 is in communication via the Internet 120, and an alternate location central provider billing system 4625 is also in communication via the Internet 120.

[0380] FIGS. 47A through 47B are transactional diagrams illustrating open, decentralized, device based mobile commerce transactions in accordance with some embodiments. Referring to FIG. 47A, the device application 4604 browses (e.g., based on the user submitting a browse request using a browser application) to transaction server 134 (e.g., a transaction web server, such as the open content transaction partner site 134). The transaction server 134 provides an offer to the device application 4604. The device application 4604 selects a purchase (e.g., based on the user's selection input). In response, the transaction server 134 seeks an API connection with the device mobile payment agent 4699, which then confirms the API connection. The transaction server 134 requests user purchase confirmation (mediated by the device mobile agent 4699 as shown), and the purchase is confirmed by the device application 4604 (e.g., based on the user's acknowledgement as similarly described above with respect to FIG. 46). The transaction server 134 then transmits a purchase receipt, and the device application 4604 confirms the receipt. The transaction server 134 then transmits the purchase bill to the device mobile payment agent 4699, which then sends the purchase bill to the device billing server (e.g., billing server 4630). The transaction server also optionally sends a confirmation of the purchase bill to the device billing server for a triangle confirmation, as similarly described above with respect to FIG. 46. The device billing server sends a copy of the purchase bill to the central provider billing system (e.g., central provider billing system 4623).

[0381] Referring now to FIG. 47B, the device application 4604 browses (e.g., based on the user submitting a browse request using a browser application) to transaction server 134 (e.g., a transaction web server, such as the open content transaction partner site 134), in which the browse request includes device ID information, such as similarly described above with respect to

FIG. 46. The transaction server 134 establishes API contact with the device mobile agent 4699, which then confirms contact and good standing for transactional purchases from the device. The transaction server 134 provides an offer to the device application 4604. The device application 4604 selects a purchase (e.g., based on the user's selection input). The transaction server 134 notifies the device mobile payment agent 4699 of the purchase description and amount, and the device mobile payment agent 4699 then requests user purchase confirmation. The purchase is confirmed by the device application 4604 (e.g., based on the user's acknowledgement as similarly described above with respect to FIG. 46), and the device mobile payment agent 4699 then transmits a purchase confirmation to the transaction server 134. The transaction server 134 then transmits a purchase receipt, and the device application 4604 confirms the receipt. The transaction server 134 then transmits the purchase bill to the device mobile payment agent 4699, which then sends the purchase bill to the device billing server (e.g., billing server 4630). The transaction server also optionally sends a confirmation of the purchase bill to the device billing server for a triangle confirmation, as similarly described above with respect to FIG. 46. The device billing server sends the purchase bill to the central provider billing system (e.g., central provider billing system 4623). In some embodiments, the communications described above with respect to FIGS. 47A-47B with the billing server and the central provider billing system are with the alternate location billing server 4632 and/or alternate location central provider billing system 4625 via the Internet 120. Similarly, in some embodiments, the transaction servers 134 are connected to the Internet 120.

[0382] Accordingly, these transaction billing embodiments do not require centralized content storage or content and transaction exchange infrastructure. For example, the transactions can be conducted over the Internet, and the user experience and content can be tailored versions of the transaction server/content provider's normal experience and content. This approach provides for a much wider array of content and transaction partners with minimal or no need to accommodate proprietary specialized systems. Moreover, the compatibility between the device billing agent transaction system and the transaction provider server is easily established, for example, by writing specifications for the header information transmitted by the device and for the secure handshake and signed message transactions that take place between the device billing agent, the transaction server and optionally the transaction server and the billing server. Once a transaction partner shows compatibility test results and concludes a business relationship with

the service provider, the service provider can place the transaction partner on the compatible and approved list and exchange security keys and/or certificates. If a common user experience is desired by the service provider across multiple transaction partners, then the experience specifications for the browser redirects can also be specified in the compatibility specification and tested before the transaction partner gains approval.

Design and Testing for Service Control

[0383] FIG. 48 illustrates a network architecture including a service controller device control system and a service controller analysis and management system in accordance with some embodiments. As described herein, the RAN gateway 410 generally represents the functionality of the various specific RAN gateway functional elements shown and/or discussed herein. For example, these RAN gateway 410 functional elements represent the gateways used to aggregate the radio access network traffic, control, charging and roaming functions and/or other functions and are shown and/or discussed herein using other terminology specific to certain industry standards, including SGSN gateway 410 and gateways 508, 512, 608, 612, 708 and 712. Although the same reference numerals are used for SGSN gateway 410 and RAN gateway 410, it will be appreciated that the RAN gateway 410 represents any or all of the RAN gateway functional elements 410, 508, 512, 608, 612, 708, 712 or any other similar industry equipment or functions depending on the embodiment. Similarly, transport gateway 420 represents the next higher level of gateway aggregation for the transport layer that is used in many networks, and this term transport gateway 420 can be interchanged with any or all of the gateways 420, 520, 620, 720 or any other similar industry equipment or functions depending on the embodiment. Those of ordinary skill in the art will appreciate which gateway description applies to a respective embodiment in which the terms RAN gateway 410, gateway 410, transport gateway 420 or gateway 420 are referenced herein.

[0384] While the embodiments described below with respect to FIGS. 48 through 63 are depicted in the context of a conventional multi-tier access network, one of ordinary skill in the art will appreciate that such embodiments can also be generalized to other network topologies including the various flattened network topologies described herein. As shown, the service controller is divided into two main functions (e.g., as compared with the embodiments of service

controller 122 depicted in FIG. 16): (1) a service controller device control system 4825 and (2) a service controller design, policy analysis, definition, test, publishing system 4835. The service controller device control system 4825 performs the device service control channel functions as previously described herein with respect to various embodiments.

[0385] The service controller design, policy analysis, definition, test, publishing system 4835 separates out the service analysis, control policy design and publishing from the device service control channel functions. The service controller design, policy analysis, definition, test, publishing system 4835 performs a variety of functions as described below. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service usage statistical analysis, notification policy or procedure response analysis and/or billing policy or procedure response analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 detects, singles out and reports device service usage, notification responses or billing behavior that is outside of expected limits but may or may not be violating policy. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service cost and profitability analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides user service control policy, notification policy or billing policy statistical satisfaction analysis for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides statistical take rate analysis for transaction offers and billing offers for single devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service.

[0386] In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service control policy definition work screens and “dry-lab” (pre-beta) testing against usage database for single devices, groups of devices, types of

devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835 provides service control policy, notification policy and/or billing policy beta testing (e.g., using beta test server 1658) in which the beta test profile is published to a subset of users or devices. In some embodiments, beta devices/users may or may not know that the service policy is being tested with them. In some embodiments, if they do know, then beta test apparatus includes offering system that provides user options to accept beta test and provide feedback in exchange for an offer (e.g., show them an offer page that comes up with their existing subscription service or ambient service – offer a free trial, a discount to something and/or reward zone points (or other incentives/rewards) if they accept the trial). In some embodiments, a beta test workstation (e.g., in communication with the beta test server 1658, such as VSP remote workstation 4920 as shown in FIG. 49) allows the beta test manager to define one or more beta test service policy, notification policy and/or billing policy control profiles. In some embodiments, the beta test workstation publishes each profile to specific individual (single) devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service. In some embodiments, the beta test workstation allows the beta test manager to analyze usage statistics, notification response statistics and/or billing/transaction offer response statistics for devices, users, groups of devices or groups of users and compare actual real-time usage versus beta test usage goals. In some embodiments, the beta test workstation allows the beta test manager to fine tune service, notification and/or billing/transaction policies and re-publish to observe changes to actual service usage until the service policy and/or notification control policies achieve the desired result. In some embodiments, the beta test workstation also allows the beta test manager to collect direct user feedback to a set of pre-designed user satisfaction or other questions regarding service usage. For example, questions can be presented through a pre-designed beta test portal or through a series of brief pop-ups that come up when the user initiates a particular action or at a particular time. In some embodiments, the beta test workstation also collects details of service and device usage (e.g., CRM data) that the beta test users have approved for collection. In some embodiments, the beta test workstation can decompose this data to determine if the users are using the service in the manner intended by the beta test goals. In some embodiments, the beta test workstation also allows for publishing multiple variants of the service and/or notification

policy control settings and compare the service usage for each group with convenient screens with information displays (e.g., statistical usage versus time of day, usage of particular activities, billing activity, device discovery activity, user response to notification message and options, user satisfaction with a particular notification policy or billing policy or traffic control policy). In some embodiments, the screens can be designed by the beta test manager.

[0387] In some embodiments, once a service is completely tested and approved for production publication, the service download control server 1660 has a workstation screen that allows the service manager to specify which group of devices are to receive the new service policy configuration. In some embodiments, the service download control server 1660 allows the service manager to define specific individual (single) devices, groups of devices, types of devices, groups of users, classes of users, or an entire set of devices and users that subscribe to a given service.

[0388] In some embodiments, a service (e.g., a newly created or new version of an existing service) is tested and/or enhanced using a new service testing model. For example, a new service (or a new version of an existing service) is loaded onto a server for testing, the new service is (optionally) tested against existing device usage statistics, a new service control definition (e.g., implemented as service processor 115 for publishing to devices 100 and a corresponding new service controller 122 for the service provider, such as a central provider or an MVNO partner, and, for example, the new service processor and service controller can be implemented using the below described SDK) for the new service is developed and possibly adjusted based on the testing against existing device usage statistics, the new service control definition is then published to beta devices (e.g., various devices 100 used for beta testing the new service), which then use the new service, service usage statistics and/or user feedback statistics are then collected (e.g., to ensure that the service is functioning properly and so that the service control definition can be tuned to ensure adequate service, user experience and for service pricing/profitability purposes), the service/service control definition is then fine tuned based on the service usage/user feedback statistics. Upon completion of the above testing and refinement of the service/service control definition, the service control definition can be published to specified groups of devices for using the new service. In some embodiments, this service control testing model for groups of devices and service partners is provided by a virtual

MVNO or VSP. For example, this allows for new services to be more efficiently and more effectively developed, tested and proliferated.

[0389] In some embodiments, service history IPDRs come from within a networking component connected to the central provider core network 110 as depicted by (e.g., real-time) service usage 118 (which as discussed elsewhere is a general purpose descriptor for a function located in one or more of the networking equipment boxes). In some embodiments, service history IPDRs are collected/aggregated (in part) from the central billing system 123. In some embodiments, service history IPDRs are collected/aggregated (in part) from the transport gateways 420. In some embodiments, service history IPDRs are collected/aggregated (in part) from the RAN gateways 410. In some embodiments, service history IPDRs are collected/aggregated (in part) from the base station(s) 125 or a networking component co-located with the base station(s) 125, a networking component in the transport network 415, a networking component in the core network 110 or from another source.

Virtual Service Provider for Service Control

[0390] In some embodiments, virtual service provider (VSP) capabilities include making available to a third party service partner one or more of the following: (1) device group definition, control and security, (2) provisioning definition and execution, (3) ATS activation owner, (4) service profile definitions, (5) activation and ambient service definition, (6) billing rules definition, (7) billing process and branding controls, (8) bill by account settings, (9) service usage analysis capabilities by device, sub-group or group, (10) beta test publishing capabilities by device, sub-group or group, and (11) production publishing, fine tuning and re-publishing.

[0391] FIG. 49 illustrates a network architecture for an open developer platform for virtual service provider (VSP) partitioning in accordance with some embodiments. As shown, the service controller design, policy analysis, definition, test, publishing system 4835 is configured so that multiple “service group owners” (e.g., the service provider for certain smart phones) or “device group owners” (e.g., eReader devices for the eReader service provider(s)) or “user group owners” (e.g., IT for Company X for their employees’ corporate mobile devices), collectively referred to as the “Virtual Service Provider” (VSP), are serviced with the same service controller infrastructure and the same (or substantially similar) service processor design

from virtual service provider workstation server 4910 and/or virtual service provider remote workstation(s) 4920. As shown, the virtual service provider remote workstation(s) 4920 communicates with the virtual service provider workstation server 4910 via VPN, leased line or secure Internet connections. The dashed lines shown in FIG. 49 are depicted to represent that, in some embodiments, the virtual service provider workstation server 4910 is networked with the service controller device control system 4825 and/or, in some embodiments, the service controller design, policy analysis, definition, test, publishing system 4835. Based on the discussion herein, it will be apparent to one of ordinary skill in the art that the VSP workstation server 4910 can also be networked in various embodiments with billing system 123, AAA server 121, gateways 410 or 420, or other network components to perform, for example, various network provisioning and activation related functions discussed herein for the device group assigned to one or more VSPs, or for other reasons as will be apparent to a given VSP embodiment.

[0392] In some embodiments, the service controller functionality is partitioned for a VSP by setting up one or more secure workstations, secure portals, secure websites, secure remote software terminals and/or other similar techniques to allow the service managers who work for the VSP to analyze, fine tune, control or define the services they decide to publish to one or more groups of devices or groups of users that the VSP “owns.” In some embodiments, the VSP “owns” such groups by virtue of a relationship with the central provider in which the VSP is responsible for the service design and profitability. In some embodiments, the central provider receives payment from the VSP for wholesale access services. In some embodiments, the VSP workstations 4910 and 4920 only have access to the service analysis, design, beta testing and publishing functions for the devices or users “owned” by the VSP. In some embodiments, the user or device base serviced by the central provider network is securely partitioned into those owned by the central provider, those owned by the VSP, and those owned by any other VSPs.

[0393] In some embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using device based service control techniques as described herein. In some embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using device assisted and network based service control techniques as described herein. In some

embodiments, the VSP manages their devices from the VSP workstations 4910 and 4920 using network based service control techniques (e.g., DPI techniques) as described herein.

[0394] For example, this approach is particularly well suited for “open developer programs” offered by the central providers in which the central provider brings in VSPs who offer special value in the devices or service plans, and using this approach, neither the central provider nor the VSP needs to do as much work as would be required to set up a conventional MVNO or MVNE system, which often requires some degree of customization in the network solution, the billing solution or the device solution for each new device application and/or service application that is developed and deployed. In some embodiments, the service customization is simplified by implementing custom policy settings on the service processor and service controller, and the custom device is quickly brought onto the network using the SDK and test/certification process. In some embodiments, the VSP functionality is also offered by an entity other than the central provider. For example, an MVNE entity can develop a wholesale relationship with one or more carriers, use the service controller to create the VSP capabilities, and then offer VSP services for one network or for a group of networks. In some embodiments, the service customization is simplified by implementing custom policy settings through the VSP embodiments on the network equipment, including, in some embodiments, service aware or DPI based network equipment that has a relatively deep level of service activity control capability. For example, using the embodiments described herein, and possibly also including some of the activation and provisioning embodiments, it is possible to efficiently design and implement custom ambient service plans that are different for different types of devices, different OEMs, different VSPs, different distributors, or different user groups all using the same general infrastructure, whether the service control policy implementation is accomplished primarily (or exclusively) with networking equipment (network) based service control, primarily (or exclusively) with device based service control or with a combination of both (e.g., hybrid device and network based service control).

[0395] As discussed herein, various VSP embodiments for performing one or more of analyzing traffic usage and defining, managing service profiles or plans, dry lab testing service profiles or plans, beta testing service profiles or plans, fine tuning service profiles or plans, publishing service profiles or plans, or other policy related settings can involve programming

settings in the network equipment and/or programming settings or software on the device. For example, as discussed herein, the service processor settings are controlled by the service controller, which can be partitioned to allow groups of devices to be controlled. As another example, equipment in the network involved with network based service control, such as DPI based gateways, routers or switches, can similarly be programmed to utilize various VSP embodiments to implement that portion of the service profile (or service activity usage control) that is controlled by network level functions, and it will be appreciated that substantially all or all of the service activity control for certain embodiments can be accomplished with the network functions instead of the device. Continuing this example, just as the device service processor settings control functions of the service processor can have a group of devices that are partitioned off and placed under the control of a VSP, various VSP control embodiments can partition off a group of devices that have service usage activity controlled by the networking equipment, including, in some embodiments, sophisticated service aware DPI based service control equipment, to achieve similar objectives. It will be appreciated that the discussion herein regarding service controller design, policy analysis, test, publishing 4835, and the discussion regarding device group, user group and other VSP related embodiments, should be understood as applicable to various embodiments described in view of device based services control, control assistance and/or monitoring, or network based services control, control assistance and/or monitoring, or a combination of device based services control, control assistance and/or monitoring and network based services control, control assistance and/or monitoring. The various embodiments described herein related to service activation and provisioning also make apparent how the programming of network equipment service control, service control assistance and/or monitoring can be implemented prior to and following activation of the device. It will also be appreciated that the VSP capabilities described herein can also be applied to those devices that have services controlled by, provided by and/or billed by the central provider, so these techniques can be applied to central provider service embodiments, MVNO embodiments and other embodiments.

Open Development System for Access Services – SDK

[0396] In some embodiments, an SDK is provided that allows developers, such as device manufacturers, service providers, MVNO, MVNE and/or VSPs, to develop various service

processors (e.g., different versions of the service processor 115) for various devices (e.g., various types of devices 100) and corresponding service controllers (e.g., different versions of the service controller 122) for various types of services and network environments. For example, a device manufacturer can use the SDK to develop a new service processor for their new device (e.g., mobile phone, PDA, eBook reader, portable music device, computer, laptop, netbook, or any other network accessible device). The device manufacturer can also preload/preinstall their new service processor on their new devices. In this example, users of the new device would then be able to utilize the new device to access network based services using the new service processor, which communicates with the deployed new service controller, as similarly discussed herein in various embodiments. For example, the device can be preinstalled with the new service processor to provide ambient services, as similarly discussed herein in various embodiments. For example, the SDK can allow for substantially similar service processors to be installed on similar and/or different devices thereby minimizing any unnecessary differences between service processor elements for device assisted services. In some embodiments, for ambient services for a group of devices, or devices associated with a certain service provider, a set of numbers (e.g., dummy numbers) can be assigned for use for attempting access via the access network using a new device that is not yet otherwise subscribed for service. In some embodiments, the set of (dummy) numbers used for ambient access by the device can also be used for associate of the device with a service provider or a type of device (e.g., eReader or some other type of network accessible device), and upon activation, the service provider assigns a real number for the activated device (e.g., which can be provided at the time of manufacture of the device, point of sale of the device, or after the point of sale of the device, such as upon activation of the device). For example, ambient access of the device can use the device ID, SIM ID, assigned phone (real or dummy) number, and/or other information associated with the device for assigning appropriate service control and service policy/profile for the device.

[0397] In some embodiments, the service processor 115 is distributed as an SDK to any device that the central provider or the VSP desires to offer services with so that the service processor 115 can be efficiently designed or adapted by the device OEM, ODM or manufacturer for operation on the service network. In some embodiments, the SDK includes either a complete set of service processor 115 agent software designed for and/or tested for the OS (Operating System) and processor set being used on the device, or a mature reference design for the OS and

processor set being used on the device, or a less mature reference design (potentially for the same OS and/or processor set or a different OS and/or processor set being used on the device) that the OEM (Original Equipment Manufacturer) ports to the desired OS or processor set, or a basic set of example software programs that the OEM or ODM (Original Design Manufacturer) can use to develop software compatible with the service, or a set of specifications and descriptions (possibly forming an interoperability standard) of how to design the software to be compatible with the service. In some embodiments, the SDK includes a set of OEM lab test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the SDK includes a set of network certification test procedures and/or test criteria to ensure that the implementation of the service SDK is compatible with the service and will operate properly. In some embodiments, the certification procedures are approved for testing by the OEM, the central provider, the VSP and/or a trusted third party. For example, the central provider is typically in control of the SDK and the test procedures, but others can be in control. In some embodiments, the test procedures are at least in part common across multiple central provider networks. In some embodiments, the SDK concept is extended to include one or more modem modules where one or more of the SDK embodiments described above is combined with a standard reference design or a standard hardware sales package for one or more modems so that the entire package forms a turn-key product that allows a device manufacturer, central provider, VSP or other entity bring new devices or device applications onto the central provider network possibly in combination with other networks in a manner that requires less engineering time and resources and less network certification time and resources than would be required in some designs that do not use this standard SDK plus module approach. For example, the standard SDK plus module product embodiments can be pre-certified and tested with one or more central providers to further reduce development time and expense. The standard SDK plus module embodiments can also use a multi-mode modem (e.g., modems based on a multimode CDMA, EVDO, UMTS, HSPA chipset as in the Gobi global multimode chipset product or modems based on other recently announced LTE plus HSPA chipsets, WiMax plus Wi-Fi chipsets or LTE plus EVDO chipsets) and a multi-mode connection manager agent so that the same SDK plus modem embodiment may satisfy a wide range of applications for many service providers around the world.

[0398] In some embodiments, at the time of manufacture, the device is associated with an MVNO. For example, the MVNO can provide an ambient service that provides a service provider clearing house, in which the device can access a network in ambient access mode (e.g., a wholesale MVNO connection through the access network) for purposes of selecting a service provider (e.g., a VSP, MVNO or carrier). Based on the service provider selection, the device credentials and/or service processor are reprogrammed and/or new software is downloaded/installed to activate the device with the selected service provider, as described herein for provisioning the device and the account on that service provider network (e.g., the ATS can track such activation, for example, for revenue sharing purposes, as an activation incentive fee).

[0399] In some embodiments ATS is implemented entirely in the network as described below. At the time of manufacture or at sometime during device distribution, the device master agent programs a unique credential in the device that cannot be re-programmed or removed (or is difficult to re-program or remove) and that can be recognized and recorded by the network at the time of activation or at some other time. In this manner, even if other, possibly primary, device credentials are reprogrammed or removed, there will still be a credential that is associated with the device master agent. The ATS process can then be implemented by using a database search function to scan through the database of activated devices to form a list of devices that have been activated for the purpose of master agent reconciliation. Example credentials that can suffice are MEID, hardware MAC address, and/or serial number, that are picked up and recorded by the service provider or other service entity at time of activation or before or after activation.

Interface Server Overlay for Billing/IPDR Feed Mediation

[0400] FIG. 50 illustrates a network architecture including a billing to service controller interface for accommodating minimum changes in existing central billing, AAA and/or other network components in accordance with some embodiments. As shown, the central billing system 123 includes a mediation, customer service and billing databases, historical usage, billing systems component 5010 and a billing to service controller interface component 5020. For example, the billing to service controller interface component 5020 allows for the central billing

system 123 to efficiently communicate with the service controller (e.g., service controller device control system 4825).

[0401] In some embodiments, an interface server (e.g., the billing databases, historical usage, billing systems component 5010 and/or the billing to service controller interface component 5020) is provided that reads the IPDRs, service profile and/or service plan information stored in the billing and/or service record database(s). In some embodiments, the interface server performs these functions in a manner that is compatible with communication formats of the billing and/or service record database(s) so that little or no changes are required in the configuration, communication formats or software of the existing central billing, AAA and/or other network components. In some embodiments, the interface server (e.g., including the billing databases, historical usage, billing systems component 5010 and the billing to service controller interface component 5020) is co-located with the central billing system components as shown, or in other embodiments, the interface server is located elsewhere. For example, the interface server can be located close to or within the components that comprise the service controller or anywhere else in the network.

[0402] In some embodiments, the interface server performs certain communication protocol translation or data format translation required to interface the information stored in the billing and/or service record database(s) to the service controller functions so that the central billing system 123 and other existing components in the network do not need to change much (if at all) to enable the service controller and service processor to implement device based/assisted service control. In some embodiments, the central billing system 123 or other network components are not required to be aware of the service control functions being implemented by the service controller or service processor, because the interface server acquires the network based information needed by the service controller and/or service processor while requiring little or no specialized awareness, communication, data formatting, user interfacing, service profile processing or service plan processing on the part of existing billing, database or networking components. In this type of overlay approach, various embodiments described herein can be used to quickly upgrade the capabilities of existing networks for new devices while minimizing the required changes to the existing network that supports legacy devices.

[0403] For example, a new ambient service plan can be implemented within the central billing system 123 that is associated with a zero or low cost billing plan and a usage limit (e.g., ambient service) that may be difficult or impossible to support in a manner that would result in high user satisfaction and a high level of control for service cost and service policy definition. Even if the central billing system 123 is not highly involved in the process, the zero or low cost plan can be implemented in a manner that results in high user satisfaction and a cost controlled service by using the service controller and/or service processor and the interface server to implement the ambient services access control, service usage control, user interface, service usage notification, transaction billing or bill by account functionality. For example, this approach can be implemented by reading the service plan and/or service policy settings for a device in the central billing database using the interface server, looking up the corresponding service policy, user notification policy, transaction billing policy and bill by account policy associated with the particular service profile or service plan, and then implementing the policies with the assistance of the service controller and/or service processor. Similarly, in another definition, multiple tiers of service control and user notification policies can be added to any number of new service profiles or service plans that would not otherwise be supported with the central billing system 123 and other network components, all with minimal or no modifications to the pre-existing network and billing system.

[0404] Another embodiment calls for receiving a standard IPDR feed from central billing 123 or another network component just like an MVNO would. For example, the interface server function can be located in the central billing system, service processor or elsewhere in the network. This provides the IPDR records for service usage policy verification and service usage notification synchronization with little or no need to modify existing billing or network apparatus.

[0405] In some embodiments, duplicate the IPDRs are sent from the network equipment to the billing system and/or network management system that are currently used for generating service billing or are used for device management or network management. In some embodiments, duplicate records are filtered to send only those records for devices controlled by the service controller and/or service processor. For example, this approach can provide for the

same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system.

[0406] In some embodiments, a bill-by-account billing offset is provided using the interface server. For example, bill-by-account billing offset information is informed to the billing system through an existing data feed and by updating the billing database using the interface server. In some embodiments, transaction billing is provided using the interface server. For example, transaction billing log information is provided to the billing system through an existing data feed and by updating the billing database using the interface server.

[0407] In some embodiments, existing/new service plan choice screens are displayed to the user, a user choice or decision/input is confirmed for a selected service plan, and then the service is implemented upon confirmation of the billing system update for the new service plan. In some embodiments, the service is implemented upon the user selection of a new service plan and then retracted if not confirmed as updated by the billing system within a certain period of time. In some embodiments, the new service plan information is updated in the billing system through an existing data feed or by updating the database using the interface server.

Integrated Service Control

[0408] FIG. 51 illustrates a network architecture for locating service controller device control functions with AAA and network service usage functions in accordance with some embodiments. As shown, an integrated device service control, AAA, device usage monitoring system 5110 is provided that integrates service controller functions (e.g., service controller device control system functions 4825 of FIG. 48) with access network AAA server 121 functions and network (e.g., real-time) service usage 118 functions.

[0409] FIG. 52 illustrates a network architecture for locating service controller device control functions in the access transport network in accordance with some embodiments. As shown, the service controller device control system 4825 is located in the access transport network 415, or in some embodiments, in the 4G/3G/2G RAN gateways 410 (as indicated by the dashed line with the arrow), or alternatively, in the 4G/3G/2G transport gateways 420 (as indicated by the dashed line with the arrow).

[0410] FIG. 53 illustrates a network architecture for locating service controller device control functions in the radio access network in accordance with some embodiments. As shown, the service controller device control system 4825 is located in the radio access network 405, or in some embodiments, in the 4G/3G base station(s) 125 (as indicated by the dashed line with the arrow), or alternatively, in the 3G/2G base stations 125 (as indicated by the dashed line with the arrow).

Ambient Services

[0411] In some embodiments, improved and simplified processes for provisioning a device or user for service on a central provider network, an MVNO network or a virtual service provider (VSP) on the central provider network are provided. In some embodiments, provisioning includes one or more of the following: a process or result of assigning, programming, storing or embedding into the device and/or network a set of credentials, or otherwise providing the credentials to the user; the credentials being at least in part carried on the device or with the user; and/or at least a portion of or a counterpart to the credentials being stored or recognized by the network so that the various network elements responsible for admitting the device access to the appropriate service activities do so once the device or user service is active.

[0412] As an example, as discussed herein, the credentials can include one or more of the following: phone number, device identification number, MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version, device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar

identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider, OEM, master agent (service distributor), VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user.

[0413] In some embodiments, provisioning includes assigning, programming or embedding into the device and/or network the information to define the level of service activity, referred to as a service profile, that the device is authorized to receive. In some embodiments, provisioning also includes establishing the device settings and/or network settings to define an ambient activation experience in which the device user receives a set of services after (e.g., within a short period of time after) purchasing or otherwise obtaining or installing the device whether the device has or has not been registered and activated with the device user or device owner.

[0414] In some embodiments, the ambient experience is the user experience that is available at the time the device is sold in the event the user has not yet signed up for a service plan. For example, the ambient experience is defined by an ambient service profile, an ambient service plan and/or the other service usage activity control policies in effect in the network, on the device, or a combination of both. For example, if the device service processor is used in large part to define the ambient service profile, then the initial provisioning and activation settings in the service processor, and possibly the service controller, can define the user service upgrade offering choices, network destination access control possibilities, traffic control policies, mobile commerce transaction capabilities (e.g., which transaction websites, WAP sites or portals the user can access to purchase information, content, music, games and/or eBooks), possibly free news or weather or other modest bandwidth Internet services that are provided free of charge to

entice the user into using/upgrading the service or using the transactions or viewing advertisements, what advertisements are displayed to the user or what advertisement based websites the user is exposed to, certain applications may have access while others are blocked (e.g., Internet based text services have access but email downloads do not), or other example service capabilities. It will be apparent to one of ordinary skill in the art that allowing all of these services, and blocking other ambient user service attempts (e.g., unpaid large file size Internet downloads or uploads or movie viewing or other access that would consume bandwidth and cause the ambient service to be a potential source of losses for the service provider) is made possible by the service profile control capabilities of the service processor and/or the service controller. The bill by account embodiments, as discussed herein, in which each service activity can, for example, be separately tracked with the service monitor and other agents and server functions to produce a billing offset that allows categorization and mediation of different billing entities (accounts) provides the capability for the service provider to individually account for the costs of each ambient service element. This allows business models wherein the free access to the end user is paid for or partially paid for by one or more service provider partners who are billed for service access using the bill by account capabilities (e.g., the transaction partners pay for user access to their transaction experience and perhaps pay a revenue share for transaction billing, the advertising sponsored website partners pay for their access service share).

[0415] While the service control capabilities of the service processor and the bill by account service cost sharing and transaction revenue sharing in some cases can create a profitable ambient business model, in other cases, the ambient services can be a potential source of losses for the service provider. Accordingly, in some embodiments, the ambient service capabilities can be modified over time to reduce service cost to the service provider or VSP based on a variety of decision factors. For example, the user can have one level of traffic control for a period of time, and if the user has not signed up for service by the end of the period, the ambient service access is reduced by changing the service control policy settings in the service processor, and the service level can be further reduced over time if the user continues to not sign up for service or the user does not create much transaction revenue. As another example, the recursive throttling algorithms discussed herein can be utilized to one or more of the service activities offered in ambient service mode so that the user experiences what full speed service is like, and if the user continues consuming appreciable bandwidth with the service activity, then

the activity is throttled back to reduce costs. In these examples, the service processor or service controller can issue the user a notification explaining that their service is currently free so their usage is being throttled, and if they desire to receive better service, service plan upgrade offers can be delivered to the UI. It will now be apparent to one of ordinary skill in the art that the various ambient service parameters, including the provisioning and activation processes used to create the ambient service activation, can also be managed by the VSP apparatus and processes described herein. For example, this allows the same service controllers and service processor solutions to be used to define a wide range of ambient experiences for various device groups or user groups that are controlled by different VSPs.

[0416] Similarly, rather than controlling the ambient service profile settings using the VSP functions to control the service controller, service processor, provisioning and activation settings, other embodiments call for the ambient service profile settings to be controlled by the network based service activity control equipment as similarly discussed herein. Depending on the level of service control and service monitoring sophistication (e.g., highly advanced DPI or service aware techniques), some, much, most or all of the above described ambient services functionality can be implemented using network based service controls and the VSP management and control embodiments described herein.

[0417] In some embodiments, a device is suspended based on inactivity, or the device is placed in a suspended service state or suspended account state, so that the network does not get bogged down with a significant number of devices and credentials that are inactive. For example, this can also result in a portion of the device credentials being assigned back to an available pool rather than reserved for that particular device (e.g., phone numbers if phone numbers are scarce). The device account and/or activation state can be re-activated when the device comes back online. For example, the suspend state can be a simple suspension of services without changing the account status, in which case the re-activation process can be automatically completed as a subset or entire set of the activation sequence that occurs when the device is initially used as described herein. The suspend state can also involve changing the account status to inactive, in which case the re-activation process can automatically reconfigure the account status back to an active state when the device re-accesses the network. For example, the suspend state can involve de-assigning or possibly re-claiming a portion of the device credentials. If a

portion of the credentials are de-assigned, then when the device re-accesses the network credentials can be automatically re-assigned as described in various embodiments described herein.

Network Based Service Monitoring, Notification and Control

[0418] In some embodiments, as described herein, it is desirable to implement some or all of the deep service usage monitoring, service control or control assistance, or service notification or notification assistance associated with a service profile in network apparatus rather than in the device, or to implement some of the deep service monitoring, control, control assistance, notification or notification assistance in the device and others in the network. This is the case, for example, in a mixed network in which some devices have some, or at least one, or all of the service processor capabilities discussed herein, but other devices do not have as much or any of the service processor capabilities. Another example is for networks or devices that do not have any service processor capabilities or where it is desirable to do all of the service monitoring, control and notification in the network rather than the device. As described below, FIGS. 54 through 63 depict various embodiments for combinations of device based service monitoring, control or control assistance, usage notification or usage notification assistance and/or network based service monitoring, control or control assistance, usage notification or usage notification assistance.

[0419] FIG. 54 illustrates a network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments. As shown, an integrated device service control, device usage monitoring system 5410 is provided that integrates service controller functions including a deep packet control (DPC) policy implementation function 5402 with access network AAA server 121 functions and network real-time service usage 118 functions. In the following discussion, it is understood that the AAA server 121 function can be re-located to another point in the network or network equipment partitioning with no loss in generality. It is also understood that many of the functional partitions described for the various embodiments within integrated device service control, device usage monitoring system 5410 can be re-drawn with no loss in applicability, function or generality. Finally, it is understood that one or more of

the functional elements described within the integrated device service control, device usage monitoring system 5410 can be removed for simplified embodiments and that not all the functionality described herein is necessary in some embodiments.

[0420] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service monitoring or control that satisfies various network neutrality and/or privacy requirements based on indication(s) received from the device or user (e.g., user input provided using the device UI using the service processor 115; user input provided through another website, WAP site or portal; or user input provided through the service contract where the user agrees to the monitoring and/or service control levels) and network based service control using a DPI service monitor 5412 and/or the DPC policy implementation 5402.

[0421] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service monitoring or service control that satisfies various privacy requirements using indication(s) received from the device or user (e.g., user input provided using the device UI using the service processor 115; user input provided through another website, WAP site or portal; or user input provided through the service contract where the user agrees to the monitoring and/or service control levels) and network based DPI service usage monitoring or DPC policy implementation using the DPI service monitor 5412 or DPC policy implementation 5402 as described below. In some embodiments, the DPI service monitor 5412 and/or DPC policy implementation 5402 include a secure database for storing service monitoring and CRM information for each device/device user. In some embodiments, the DPI service monitor 5412 and/or DPC policy implementation 5402 can be integrated with the integrated device service control, device usage monitoring system 5410 (as shown) or provided within a separate router, server, and/or software/hardware implemented function that is in secure communication with the integrated device service control, device usage monitoring system 5410 and/or other network elements based on the network architecture. In some embodiments, a secure data store, such as a secure database, is not integrated with the DPI service monitor 5412 or DPC policy implementation 5402 but is in secure communication with the DPI service monitor 5412 or DPC policy implementation 5402, the integrated device service control, device usage monitoring system 5410 and/or other network elements depending on the architecture

(e.g., a billing server or any other network element). In some embodiments, the user selects limits and/or restrictions on who can access remotely stored service usage history and/or other CRM/privacy related data (e.g., CRM/privacy gatekeeper settings), and, for example, other network elements and/or network administrators access to such data can be limited and/or restricted accordingly. For example, access to such stored service monitoring and CRM information can require certain security credentials and/or using various other well known secure data storage techniques, such as the various secure storage techniques described herein.

[0422] In some embodiments, the secure database possessing user service usage information that is considered sensitive and has not been approved for distribution by the user can be made unavailable to the credentials possessed by network managers or network functions except, for example, for emergency service situations of government mandated monitoring needs where special credentials are brought out of secure storage that are not normally available. In some embodiments, rather than the user selecting limits, a certain set of restrictions are assumed unless the user selects information filtering settings that allow more information to be shared with the network functions, network administrators or service provider partners. In some embodiments, the information is filtered to remove information thought to be sensitive but still transmits service usage information needed for monitoring network services or other important parameters. For example, the website destinations a user is visiting can be classified with generic identifiers that are not decodable or the individual website information can be completely removed. Many other examples will be apparent to one of ordinary skill in the art.

[0423] For example, the stored service monitoring and CRM information can also be organized into groups to define group CRM profiles to store service monitoring information for every user indexed by the user credentials (e.g., such groups can also be used for various VSP related functions, as described herein). The DPI service monitor 5412 or DPC policy implementation 5402 also uses the secure storage to store service monitoring information for each user indexed by the user credentials or another aspect of the device identifier or address assignment (e.g., IP address or MAC address). In some embodiments, a CRM information manager (e.g., a supervisor program executing on the integrated device service control, device usage monitoring system 5410) communicates with the other network functions and provides filtered service usage and CRM information according to CRM filtering rules for each user or for

groups of users. In some embodiments, the filtered CRM data can be made available using secure communications with other networking equipment by the integrated device service control, usage monitoring system 5410. In some embodiments, the filter settings for some users allow more information to be shared from the secure service usage information than others due to the differences in user preference settings and/or service plan agreements.

[0424] In some embodiments, user privacy preference information is used to determine the privacy filter settings, which are securely implemented by the integrated device service control, device usage monitoring system 5410. For example, service CRM filter settings can be received at the time of service contract sign up (e.g., service plan selection) and/or allow the user to log into service preferences web page to change settings (e.g., without involving any interaction with local software on the device). As another example, software on the device (e.g., including the service processor 115) can be used for selecting user CRM/privacy preferences, which are securely communicated to the integrated device service control, device usage monitoring system 5410 (e.g., the device can include credentials that can be verified to allow for selection/modification of CRM/privacy preferences or other user based preferences securely maintained in a network server, such as the integrated device service control, device usage monitoring system 5410 or another network element, such as shown in various other embodiments described herein). In these examples, the filtered CRM data is available from the integrated device service control, device usage monitoring system 5410 for other network components over a secure or open communication link. In another example, user CRM/privacy preferences are input using a web server hosted by the integrated device service control, device usage monitoring system 5410 or the central billing system 123. In another example, software on the device (e.g., including the service processor 115) can be used for securely communicating user preference decisions to an intermediate server that acts as a device manager and intermediate server for devices or device groups and the integrated device service control, device usage monitoring system 5410.

[0425] In some embodiments, the integrated device service control, device usage monitoring system 5410 provides for network based service control as described below. In some embodiments and similar to the above described network based CRM filtering embodiments, the DPI service monitor 5412 or DPC policy implementation 5402 includes secure storage (e.g., a

secure database) for storing service monitoring information (e.g., based on user selections/preferences), and the DPC policy implementation 5402 performs traffic shaping/throttling algorithms for each user based on the stored service monitoring information from DPI service monitor 5412. For example, network based DPI traffic inspection by the DPI service monitor 5412 can use the secure storage to save service monitoring information for each user indexed by the user credentials or other parameters, such as IP address or other network tag. As another example, the DPC policy implementation 5402, for example, which can be supervised by policy management server 1652 as described herein with respect to various other embodiments, can implement service usage history statistical analysis inside the secure storage and maintain a service usage history analysis for each device/user and/or perform various traffic shaping and/or throttling algorithms based on various device, user selected and/or service plan related settings (e.g., for network neutrality purposes) allowing for various higher level service usage goals for one or more users, as similarly described herein with respect to various device based service usage monitoring embodiments (e.g., except for certain encrypted network traffic flows or application related flows for which traffic control generally needs information from the application level and/or content specific traffic control).

[0426] In some embodiments, input is collected on how to implement service control (e.g., from the user of the device). For example, such input can be determined based on one or more of the following: a service plan choice for the device; input provided by a user via a website (e.g., web based portal) for indicating changes to service control policies, as similarly described above; input provided by a user via the device (e.g., including the service processor 115), which securely communicates the input to the DPC policy implementation 5402, for example, which can be supervised by the policy management server 1652; and input provided by a user via the device (e.g., including the service processor 115), which securely communicates the input to an intermediate server for the DPC policy implementation 5402, as similarly described above. In some embodiments, such service control is based on various algorithms as described herein that identify the heaviest usage service activities and recursively control the speed for those activities while leaving certain others unaffected, and in a manner that is specified or selected by the user to ensure network neutrality. In some embodiments, the user is offered a choice for controlling service usage and/or selects an algorithm that controls all activities equally/neutrally (e.g., based on selected user preferences). For example, by

implementing service control algorithms that are network neutral (e.g., throttling all activities equally or throttling the highest usage algorithms without singling out certain activities for throttling unless they satisfy certain network neutral usage history or usage statistics criteria), or that are approved, selected or otherwise specified by the user, network neutral traffic control or service usage control can be maintained.

[0427] In some embodiments, the DPI service monitor 5412, possibly in conjunction with the service usage notification 5420 and/or service history server 1650, provides service usage/service cost (e.g., a real-time service usage counter) related notifications to the device based on user preferences, as similarly described above with respect to various device based service usage/service related notification embodiments. For example, the DPI service monitor 5412, for example, in conjunction with the service usage notification 5420 and/or service history server 1650, can perform service usage/service related notification algorithms based on one or more of the following: service plans, device settings, and/or user selected preferences (e.g., such notification messages can be securely communicated to the device and/or to the device via an intermediate server). For example, the policies that govern how the user is notified of service usage or service cost can be determined by the policy management server 1652 and/or the service usage notification 5420. As another example, user acknowledgements of important notification messages and/or user choices related to important service usage decisions can be requested, as similarly discussed above with respect to device based service usage/control embodiments, which can then be communicated to the central billing system 123 as confirmation for any such important notification messages (e.g., related to service usage overage charges and/or confirmation of service upgrades). In some embodiments, various other service usage algorithms related to service usage and/or service cost forward projections described herein with respect device based service usage forward projection embodiments are performed in the network, such as by the integrated device service control, device usage monitoring system 5410, and such forward projections can then be communicated to each respective device as service usage notification messages (e.g., using a push based approach (initiated in the network) and/or pull based approach (initiated by a request from the device)). For example, these embodiments for projected service usage methods, as described herein, can be helpful for determining when the user is using services in a manner that will cause the user to run over a service limit so that

the user can be notified, or the service can be controlled or throttled if the user has selected a control or throttling option.

[0428] In some embodiments, one or more intermediate servers are provided for workload balancing and/or off-loading the integrated device service control, device usage monitoring system 5410 and perform one or more of the functions described above with respect to various embodiments of the integrated device service control, device usage monitoring system 5410. In some embodiments, service plans, device settings, and/or user selected preferences are used to associate each device/user with a preprogrammed profile to more efficiently associate such devices/users with their selected service plans, device settings, and/or user preferences. For example, the process of setting a service profile for a given device can be determined by assigning the device to a service flow that has the pre-defined service profile and is shared with other devices within the integrated device service control, device usage monitoring system 5410 rather than individually processing the service flow manipulations for each device. In some embodiments, the act of provisioning and activating a service profile for a given devices involves setting up the service flow definition and identifier within the integrated device service control, device usage monitoring system 5410 (if it is not already set up) and then assigning the routing of the device credentials to that service flow identifier. User preferences can, for example, be accounted for by assigning the device service flow to one of several pre-defined profiles based on user preferences that are all supported under the same service plan. For example, one service flow profile can call for service usage notification but no control under the same service plan as another service flow profile that calls for less notification but active service usage control to maintain user costs to a monthly post-pay limit.

[0429] In some embodiments, the bill by account function is implemented in the context of the integrated device service control, device usage monitoring system 5410 or other network based system embodiments described herein. For example, the DPI service monitor 5412, in some cases in conjunction with service history server 1650, can operate in conjunction with bill by account policy settings stored in the billing event server 1662 so that service activities are divided into the account classifications defined by the service profile settings. The bill by account feeds can then be sent to the billing system or to an intermediate billing event aggregation server that collects this type of deep packet inspection generated information from

one or more integrated device service control, device usage monitoring system 5410 units to aggregate and format the information in a manner that may be used by the central billing system 123. In some embodiments, the bill by account information collected in a network box like the integrated device service control, device usage monitoring system 5410 is augmented by bill by account information collected on the device as described herein, and any intermediate server that can be used to aggregate and format these bill by account feeds for the central billing system deals with both types of data, from the network and from the devices.

[0430] As shown in FIG. 54, in some embodiments, integrated device service control, device usage monitoring system 5410 includes the service control server link 1638, which, for example, can be used as described above (e.g., with respect to FIG. 16 and other embodiments described herein) to communicate with device service processors 115. In some embodiments, billing server 1662 within integrated device service control, device usage monitoring system 5410 detects service usage events reported by DPI service monitor 5412, in some cases in conjunction with service history server 1650, generates a billing event that can be recorded or transmitted to the central billing system 123. In some embodiments, billing server 1662 receives information from device billing agent 1695 and/or device service monitor agent 1696 and transmits the device service usage billing events to the central billing system 123. In some embodiments, certain billing events that are advantageously collected in the network (e.g., DPI service monitor 5412 and/or billing event server 1662) are combined with certain billing events that are advantageously collected on the device (e.g., service monitor agent 1696 and/or billing agent 1695), and both sources of billing information are transmitted to the billing system 123. Similarly, in some embodiments, certain service usage information is collected with service usage monitor agent 1696, and that information is combined with service usage information collected from DPI service monitor 5412 and/or service history server 1650 and/or service usage 118. In some embodiments, certain service aspects are controlled using network based DPC policy implementation 5402, in some cases in conjunction with or supervised by network based policy management server 1652, and other service aspects are controlled using device based policy implementation agent 1690, in some cases in conjunction with or supervised by policy control agent 1692. As will now be apparent to one of ordinary skill in the art in view of the numerous embodiments described herein, many hybrid approaches to service usage monitoring, service control, service notification or service billing can be accomplished with some aspects of

the policy, notification, control, monitoring or billing being implemented/performed on the device apparatus described herein and others implemented/performed on the network apparatus described herein. The presence of access control integrity server 1662 and many other service control verification embodiments described herein make it apparent that the integrated device service control, device usage monitoring system 5410 embodiments also provide for affirmative verification of whatever functions are implemented on the device. It will also be apparent that all of the above combinations of device and network functions, and many others, can be accomplished in ways that are network neutral and/or protect user privacy preferences by implementing the service control algorithms in a network neutral manner and/or receiving user preference input on how to implement service control, and by maintaining service usage and CRM information security and filtering on both the device 100 and the network based integrated device service control, device usage monitoring system 5410.

[0431] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates or plays a part in automated provisioning and activation of the devices as similarly described above with respect to various device based automated provisioning and activation embodiments. In some embodiments, the activation server 160 is integrated into or partially integrated into device service control, device usage monitoring system 5410.

[0432] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates ambient services as similarly described above with respect to various device based ambient services embodiments.

[0433] In some embodiments, the integrated device service control, device usage monitoring system 5410 facilitates VSP and ODI solutions as similarly described above with respect to various device based VSP and ODI embodiments.

[0434] Various other network architectures for network based service control including deep packet inspection functions can similarly be used as will be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[0435] FIG. 55 illustrates another network architecture for locating service controller device control functions with AAA and network service usage including deep packet inspection functions in accordance with some embodiments. As shown, the service processor 115 is not present on the devices 100, and the integrated device service control, device usage monitoring system 5510 performs all service monitoring, service control, billing, and notification functions.

[0436] FIG. 56 illustrates a 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments. As shown, a 4G/3G/2G DPI/DPC enabled gateway 5610 (e.g., implemented in either gateway 420 or gateway 410 or a combination of both) where the conventional service gateway functions 5616 (e.g., routing, switching, protocol translation/tunneling, charging data function (CDF), charging gateway function (GCF), mobility management, and/or suspend/resume) are combined with one or more of the following embodiments and integrated into one or a combination of the service gateways (e.g., RAN and/or transport gateways): DPI service monitor 5412, service history server 1650, device usage 118, DPC policy implementation 5402, policy management server 1652, user notification 5618, billing event server 1662, access control integrity server 1654, service control service link 1638, data plane I/O 5612 (e.g., used to represent the I/O port(s) for the gateway), and/or DPI/DPC gateway control plane link 5622 (e.g., used to represent the control plane network channel connecting the above elements to other network equipment and in communication with gateway control communication 5620). The packet processing architecture shown in this figure calls for a multi-point to multi-point backplane bus scheme, but it will be apparent that other data path configurations are possible including serial. As will also be apparent, the above described configuration can also be applied to either the transport gateway 420 and/or the RAN gateway 410. As mentioned above, it is possible to maintain a secure storage on the 4G/3G/2G DPI/DPC gateway 420 or 410 that requires secure credentials to get into so that user privacy is protected and service usage information or CRM information is filtered according to user preferences prior to sending to another network function or network manager, and the same allowances can also be applied for emergency or government monitoring purposes. Network neutrality can also be maintained in this configuration by maintaining network neutrality in the service control algorithm and/or soliciting user input on how to control service usage just as discussed above for other network service control implementations or as discussed in the device based service control descriptions.

[0437] In some embodiments, the bill by account function is implemented in the context of the 4G/3G/2G DPI/DPC gateway 5610 embodiment or other network based system embodiments described herein. For example, the bill by account information can be completely derived from the network box (e.g., 4G/3G/2G DPI/DPC gateway 5610) without assistance from device based service monitoring or billing capabilities, or none may exist on the device. In this example, the DPI service monitor 5412, in some cases in conjunction with service history server 1650, can operate in conjunction with bill by account policy settings stored in the billing event server 1662 so that service activities are divided into the account classifications defined by the service profile settings. The bill by account feeds can then be sent to the billing system or to an intermediate billing event aggregation server that collects this type of deep packet inspection generated information from one or 4G/3G/2G DPI/DPC gateway 5610 units to aggregate and format the information in a manner that can be used by the central billing system 123. In some embodiments, the bill by account information collected in a network box, such as the 4G/3G/2G DPI/DPC gateway 5610, is augmented, refined or otherwise added to by bill by account information collected on the device as described herein and any intermediate server that can be used to aggregate and format these bill by account feeds for the central billing system deals with both types of data, from the network and from the devices.

[0438] FIG. 57 illustrates a network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420 in accordance with some embodiments. As shown, the VSP workstation server 4910 is in communication with the 4G/3G/2G DPI/DPC gateways 410 and/or 420, the Service Controller Design, Policy Analysis, Test, Publishing System 4835, and/or other networking elements including possibly the central billing system 123, the mobile wireless center 132 (HLR) and/or the AAA server 121 for the purpose of provisioning and/or controlling settings in the 4G/3G/2G DPI/DPC gateways 410 and/or 420, the mobile wireless center 132 and possibly other equipment for the purpose of implementing a portion of the VSP open partner functionality discussed herein. In FIG. 57, the 4G/3G/2G DPI/DPC gateway 5610 functionality as shown in FIG. 56 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420 as similarly described above. For example, the VSP functionality can also be used to set higher level policies associated with the 4G/3G/2G DPI/DPC gateway 420 or 410, such as provisioning or activation profiles or policies, ambient service profiles or policies, and/or bill by account

service profiles or the other higher level service profile or service plan embodiments discussed herein. In some embodiments, the provisioning and/or activation steps described herein involve setting service policies in the 4G/3G/2G DPI/DPC gateway 420 or 410. In some embodiments, ambient services or ambient activation involve setting up service profiles within the 4G/3G/2G DPI/DPC gateway 420 or 410 that allow the desired activities and block the undesired activities. For example, these settings can be included as part of the open service provider partner programming capabilities of the VSP workstation server 4910 embodiments.

[0439] FIG. 58 illustrates another 4G/3G/2G DPI/DPC enabled gateway in accordance with some embodiments. As shown, a 4G/3G/2G DPI/DPC gateway 5810 (e.g., implemented in either gateway 420 and/or gateway 410) is provided in which the service processor connection (e.g., via service control server link 1638 as shown in FIG. 56) is not present so that all service monitoring, control, billing event collection and transmission, and notification are performed by the 4G/3G/2G DPI/DPC gateway 5610 (e.g., gateways 410 and/or 420).

[0440] FIG. 59 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, the AAA 121 and the mobile wireless center 132 in accordance with some embodiments. As shown, FIG. 59 provides a network diagram corresponding to FIG. 58, with similar functionality to the embodiment shown in FIG. 57, in which the service processors 115 are not present on the devices 100. In FIG. 59, the 4G/3G/2G DPI/DPC gateway 5810 functionality as shown in FIG. 58 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420 as similarly described above.

[0441] FIG. 60 illustrates a 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments. In some embodiments, enhanced network based service monitoring, control, billing and notification as discussed above is implemented using a 4G/3G/2G DPI/DPC enabled gateway 6010 and service controller device control system 6025 as shown. In some embodiments, the functions shown in the figure to be inside of the service controller device control system 6025 have been moved from the 4G/3G/2G DPI/DPC gateway 5610 of FIG. 56 (e.g., or from gateways 410 and/or 420) so that they reside in a separate server embodiment or other network equipment function separate from the 4G/3G/2G

DPI/DPC gateway 6010. For example, this architecture can be used when the network equipment manufacturer desires to separate these functions or has an existing product that it is desirable to upgrade by adding a separate box. As another example, this architecture can be used when the 4G/3G/2G DPI/DPC gateway 6010 is not capable of keeping up with large numbers of individual user profiles so it is desirable to go to a scalable server configuration in which load balancing can be applied with a potentially more flexible programming environment for implementing service policy management functions, statistical service history analysis algorithms, service usage projection, and/or service control (or throttling) algorithms. In some embodiments, a secure storage is provided on the 4G/3G/2G DPI/DPC gateway 6010 and/or the service controller device control system 6025 that requires secure credentials to get into so that, for example, user privacy can be protected and service usage information or CRM information can be filtered according to user preferences prior to sending to another network function or network manager, and the same allowances can also be applied, for example, for emergency or government monitoring purposes. For example, network neutrality can also be maintained in this configuration by maintaining network neutrality in the service control algorithm construction and/or soliciting user input on how to control service usage just as discussed above for other network service control implementations or as discussed in the device based service control descriptions.

[0442] FIG. 61 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, AAA 121 and mobile wireless center 132 in accordance with some embodiments. In FIG. 61, the 4G/3G/2G DPI/DPC gateway 6010 functionality as shown in FIG. 60 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420, as similarly described above, and which are in communication with the service controller device control system 6025 as shown.

[0443] FIG. 62 illustrates another 4G/3G/2G DPI/DPC enabled gateway and service controller device control system in accordance with some embodiments. As shown, the capability to communicate with the service processor 115 has been removed so that all service monitoring, control, billing event collection and transmission, and notification are performed by the 4G/3G/2G DPI/DPC gateways 6210 (e.g., implemented in gateways 410 and/or 420) in

conjunction with the service controller device control system 6225 without assistance from the service processors 115.

[0444] FIG. 63 illustrates another network architecture including the VSP workstation server 4910 in communication with the 4G/3G/2G DPI/DPC gateways 410 and 420, AAA 121 and mobile wireless center 132 in accordance with some embodiments. In FIG. 61, the 4G/3G/2G DPI/DPC gateway 6210 functionality as shown in FIG. 62 is implemented in the 4G/3G/2G DPI/DPC RAN gateway 410 and/or the 4G/3G/2G DPI/DPC transport gateway 420, as similarly described above, and which are in communication with the service controller device control system 6225 as shown.

[0445] As will be apparent to one of ordinary skill in the art, the above described embodiments can be extended to include some or all of the functions depicted in the 4G/3G/2G DPI/DPC service gateways of FIG. 56 in the base station or base station controller 125.

Provisioning and Activation

[0446] In some embodiments, automated provisioning and activation includes automation of one or more of the following functions: (1) programming device credentials or partial credentials and recording them in a database (or providing same when they are programmed into the device), (2) associating these credentials with the proper provisioning and/or activation actions to be taken on the device and in the network, (3) directing the device to the proper activation function (e.g., activation server) sequence when it attempts to connect to the network, (4) completing provisioning of the device, (5) programming the AAA, billing system, gateways, mobile wireless center and other network equipment to the proper initial device service control settings, and (6) establishing a service account for the device.

[0447] In some embodiments, improved processes for activating service for a device or user with a network service provided by a central provider network, an MVNO network or a VSP on the central provider network are provided. In some embodiments, activation includes one or more of the following: a process or result of associating a service account with device or user credentials; with the service account potentially further being associated with a service profile defining the service activities that the device is authorized to access; creating or updating

a service usage or billing record and associating it with the service account to create a service plan; and/or initiating service to the device or user in which the network equipment allows access to the appropriate level of service activities. In some embodiments, VSP embodiments include the provisioning and activation apparatus embodiments of any or all forms.

[0448] In conventional mobile device provisioning systems, the provisioning and activation process required to create a user service account and enable the device to access the desired level of service activities can limit mass market, low cost or user friendly applications of the device or service, because the process can often be cumbersome, time consuming and/or expensive for the service provider, service owner, master agent (service distributor), MVNO, VSP and/or user. Accordingly, the various embodiments for provisioning and activation described herein simplify the provisioning and activation process for mobile devices. In some embodiments, provisioning and activation for the device and/or the network accommodates a wide variety of device types and service profile types, with the capability to perform the provisioning and activation at a number of points in the manufacturing, distribution, sales and usage progression for the device, and the ability to either pre-activate before first device use or very quickly activate during first device use (or during some later use of the device).

[0449] In some embodiments, as described herein, the term provisioning generally refers to those actions/processes associated with programming the device with credentials or other device settings or software installations used to later activate the device, as well as, in some embodiments, creating database entries and other credential associations in the network so that the network and/or device have the information used to recognize the device or credentials and implement the service policies in the service profile and/or service plan once the service profile and/or service plan are activated. In some embodiments, as described herein, the term activation generally refers to the process of creating or selecting the service plan and/or service profile, programming the settings that are used in each (e.g., required) network function and/or each (e.g., required) device function so that the system can properly associate the device credentials with the appropriate service activity policies, and then admitting the device onto the network. The term activation can also refer in some embodiments to the creation of a user or device service account, in some cases, with user or device owner information or billing information. In some embodiments, the process of provisioning amounts to assigning credentials to the device

and programming a portion or all of the credentials on the device, entering a portion or all of the credentials in the various necessary network equipment databases so that the network components are capable of identifying the device and associating it with the network based portion of the admission, traffic processing, service monitoring, billing, service limits and other policies that are eventually defined by the service profile and service plan.

[0450] Further examples of the network based service profile policies include network access level, traffic routing, service monitoring, service limits and actions taken upon reaching service limits. Once the service profile is created and activated during the activation process, the device credentials and the associated service profile are communicated throughout the necessary network elements so that each element can implement its part of the network portion of the service profile policies. This process of propagating the service profile settings to all the required network equipment components is a portion of what is referred to herein as activation in accordance with some embodiments. In some embodiments, the activation process includes associating the credentials with the proper service plan and/or service profile, and possibly completing the process of programming the device functions and/or network functions so that the device can be admitted to the appropriate level of network services. In some embodiments, activation also includes the service processor software settings, configurations or installs for each function or agent in the service processor to implement its part of the service profile, service plan, service billing or transaction billing policies. In some embodiments, activation also includes the creation of entries in the various service account databases and/or billing databases to create a user account or device owner account for the purpose of managing the user choices for service plan and other account information storage and management aspects, such as maintaining status information, maintaining the central service profile configuration, conducting reconciliation and billing exchanges, service usage history, and/or account history.

[0451] In some embodiments, the term credentials generally refers to the set of information parameters that the network and/or device uses (e.g., requires) to admit the device onto the network and associate it with the appropriate service profile and/or service plan. For example, the credentials can include one or more of the following: phone number, device identification number, MEID or similar mobile device identifier, hardware security device ID, security signature or other security credentials, device serial number, device identification and/or

credential information via security hardware such as a SIM, one or more IP addresses, one or more MAC addresses, any other network address identifier, embedded device descriptive information block (static or programmable), security key, security signature algorithms, passwords or other secure authorization information, service processor (or similar device client or agent software) identifier or settings or version, device type identifier, browser (e.g., http, https, WAP, other browser client) header information or similar identifier, browser token information or similar identifier, browser cookie information or similar identifier, embedded browser instructions, portal-client (e.g., interface or communication agent that connects to a network portal used at least in part for provisioning or activation for the device or by the user) header information or similar identifier, portal-client token information or similar identifier, portal-client cookie information or similar identifier, embedded portal-client instructions, service provider, OEM, master agent (service distributor), VSP, device service owner identifier, distributor or master agent, and/or any information the network can use to authorize network admission, provision the device, provision the network, activate service, authorize, associate or enable the device with a provisioning sequence, associate or enable the device with one or more service profiles, associate or assist the device with an activation sequence, associate or enable the device with an ambient profile or service experience, associate or enable the device with one or more service plans or service capabilities, associate the device with a service provider or service owner, associate the device with an OEM or master agent, associate the device with a distributor or master agent, or associate the device with a device group, user group or user. In some embodiments, at least some of the credentials are unique to the device, and, in some embodiments, groups of devices share one or more aspects of the credentials. In some embodiments, the term permanent credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a permanent basis. In some embodiments, the term temporary credentials generally refers to the set of credentials that include at least a subset that are intended to be assigned to a device or user on a temporary basis. In some embodiments, temporary credentials are eventually replaced by permanent credentials. In some embodiments, at least some elements in the temporary credentials (e.g., phone number and/or access or authorization security credential) are used for more than one device. In some embodiments, the temporary credentials are recycled from one or more devices and used for one or more other devices, for example, when they remain unused for a period of

time or when they are replaced with permanent credentials on one or more devices. It should not be inferred from the term permanent credentials that permanent credentials are never recycled, for example, when the user discontinues service or use of the credentials. Also, the term temporary credentials does not imply that temporary credentials are always temporary. In some embodiments, partial credentials or pre-activation credentials generally refer to a subset of credentials that are to gain access to limited network services for the purpose of provisioning of credentials and/or activation of a service plan or service profile. For example, prior to a phone number being assigned, a device can gain access to a limited set of network server destinations in which embedded information contained in the device (e.g., the partial credentials) is provided to the server, the server associates that information with the proper additional credentials (including the phone number) to assign to the device and/or associates the information with the proper service profile to activate service. In this example, partial credentials can include device type, OEM, service provider, VSP, device identification number, SIM, service processor configuration or some other information used by the server to determine what the credentials should be and the proper service profile.

[0452] In some embodiments, a permanent service account generally refers to the service account that is permanently associated with the user and/or device. For example, this account includes an association with the device or user credentials, user information or billing information, service profile, billing profile, network authorization status and other aspects that define the device or user service policies and billing policies. In some embodiments, the term temporary service account generally refers to a service account that is temporarily set up and associated with the device before some or all of the required permanent account information is available or entered for a device or user. For example, this account can be set up with an association with an actual user, or can be set up with a mock user or unassigned user association so that the network and billing system can recognize the credentials, authenticate the device, admit the device, provide the proper level of service activity control according to the service profile associated with the temporary service account, or collect the service activity usage information for various network and billing system accounting needs before actual user information or billing information has been entered into the network systems. For example, a temporary service account can make it possible or easier to use existing billing systems or other network systems to provide simplified provisioning, simplified activation or ambient services. A

temporary service account can also become a permanent service account by replacing mock user or unassigned user information with actual user information, or a temporary service account may need to be replaced by a permanent service account when actual user information needs to be entered into the network systems, possibly including the billing or service profile databases.

[0453] In some embodiments, temporary or permanent device credentials and other information used/required for provisioning the device are generated with apparatus located at the manufacturer or in the distribution channel as discussed below. In some embodiments, the apparatus includes a local onsite server that typically shares some aspects of the provisioning information (e.g., phone number, phone number range, MEID or MEID range, SIM number or SIM number range, IP address or IP address range, MAC address or MAC address range, other secure device credential elements) with a network provisioning database. In some embodiments, the apparatus includes a server terminal, and the aforementioned portion of the credentials is generated by the network and shared with the local provisioning apparatus. In some embodiments, as will be discussed below, the provisioning credentials are in part generated in the network and shared with the device while it is connected online to an activation server (e.g., activation server 160) that is connected to the access network. Similarly, there can be activation servers connected to apparatus in the manufacturing or distribution channel that service device activation, or over the air or over the network apparatus connected to an activation server, which in turn connects to the device, can be used to accomplish activation programming of the network and device as further discussed below.

[0454] In some embodiments, when a device is provisioned and entered into the network provisioning database, it is associated with the automatic provisioning and/or activation sequence the device is intended to go through once it connects to the network or to the apparatus that will complete the process. In some embodiments, one or more device parameters (e.g., service owner, device type, OEM, plan type, IP address, security credential and/or software version) are used to determine what the appropriate network provisioning steps and/or settings are for completing the provisioning and/or activation process, and this association information is stored in the network provisioning database for propagation of the provisioning profiles or activation profiles to the various network equipment elements. In some embodiments, the network provisioning database is provided (e.g., in the network) that associates the pre-activation

provisioning information (e.g., generated, as described herein, at time of manufacture, sometime during distribution, by the user on a website by a sales associate or other activation assistant, or by the network when a new device enters the automatic activation process). For example, the pre-activation provisioning information informs the network whether or not to let the device onto an activation sequence when the device attempts access, and in some cases, also instructs the network to direct the device to a specific activation sequence including, for example, an activation server (or other activation sequencing apparatus) sequence as described herein. In some embodiments, a central database is queried by other network equipment or the central database is included in one or more of the network elements (e.g., the AAA server and/or billing system, mobile wireless center 132), or the database is copied in part or in whole in various network elements (e.g., the central database, AAA server, mobile wireless center, billing system and/or gateways).

[0455] In some embodiments, propagating the network equipment provisioning information for a given device or group of devices is accomplished with a network provisioning system that has access to the network provisioning database and is capable of programming the appropriate network equipment. In some embodiments, this network equipment is referred to as “network management” equipment or “network provisioning” equipment. In some embodiments, there are several functions that take part individually or in concert, including, for example, the AAA server 121, service controller 122 (either with device based/assisted services through the service processor related embodiments or with network only embodiments as described herein), the mobile wireless center 132 (e.g., including the home location register (HLR) or other similar function referred to by other industry terms), the activation server(s) 160, other network provisioning or management equipment attached to or associated with the billing database system, and/or some other equipment apparatus. In some embodiments, the local database on the device, database in the AAA server and/or database elsewhere in network is provisioned to inform the gateway of the process for handling the pre-provisioned device according to, for example, the credentials. For example, if the device is not recognized or not authenticated onto the access network as an activated device with associated active service profile and/or service plan, the device connection or communication can be directed (or routed) to a generic activation server that provides an activation sequence that is not necessarily determined by one or more of the specific device credential elements, partial credential elements,

device profile or partial device profile that define something specific about the activation sequence for the device. In another example, in which the device is not recognized or authenticated as an activated device with associated service profile and/or service plan, the device can be directed (or routed) to an activation service (or other activation sequencing apparatus) that uses some part of the credentials or range of partial credentials or a portion of a partial or complete device profile to determine a desired pre-determined device specific or device group specific activation sequence that is implemented by a specific activation service sequence or other activation sequence apparatus. In another example, in which the device is not recognized or authenticated as an activated device with associated active service profile and/or service plan, a portion of the device credentials or partial credentials can be used as a look-up index into a database that determines what the specific device activation sequence should be, and the device can be directed (or routed) to a specific activation server sequence or other activation sequencing apparatus.

[0456] In some embodiments, a database in the AAA server or database elsewhere in network is provisioned to inform the gateway what to do with a pre-provisioned device according to the credentials. For example, devices can be authenticated (for activated devices), routed to activation servers (or other activation sequencing apparatus) or denied access. In some embodiments, the AAA server (and/or other network elements) provide the above discussed look-up function for the above gateway description in which a lookup database, locally stored or stored in a central database, is queried to provide secondary routing information to the specific or generic activation servers.

[0457] In some embodiments, the pre-provisioned database is located in the billing system. In some embodiments, the billing system accesses the pre-provisioned database (e.g., stored on the billing system or another network element) for the purpose of setting up temporary accounts or permanent accounts and associating those accounts with pre-activation status, activated free ambient or activated paying customer.

[0458] In some embodiments, for zero activation, all the required pre-provisioning or programming of the above network elements, or others, is coordinated by the network provisioning system at some point after the partial or full device credentials have been associated

with the device or reserved for a particular device type or service type. In some embodiments, the network provisioning system also coordinates the information to or from the device provisioning apparatus that is described elsewhere.

[0459] In view of the various embodiments described herein, it will be appreciated that many of the automated or background provisioning, activation and ambient embodiments described herein can be accomplished with network based approaches, device based approaches, or network/device combination/hybrid based approaches. For example, when the access control for the provisioning process is accomplished in the device (e.g., a device based approach), the activation server can be located anywhere on the Internet, and the device will ensure that the activation process is conducted with the activation server while blocking other traffic from occurring. As another example, some or all of the ambient provisioning programming steps become steps to program the access control, traffic control, application control, bill by account rules, and/or other aspects in the service processor or service controller as described herein.

[0460] In some embodiments, the provisioning apparatus described herein can be a computer located in the user's home or business, and the user or an IT manager has access to a website that provides the provisioning information, in which the computer serves as the provisioning or software programming apparatus. In some embodiments, the network itself, possibly through an activation server 160, website or other interface to the device, becomes the provisioning apparatus, in some cases, with the assistance of software on the device to affect the programming of provisioning information from the network or the communication of device credentials or other information to the network. For example, this software can be a background process that runs without user interaction, a portal/widget program, a web browser based program, a WAP browser based program, and/or any other program that provides a counterpart function to the network functions effecting the provisioning (e.g., activation server). In some embodiments, the activation server either initiates a specific provisioning sequence if device software is present to assist or routes to a website for manual entry if there is no software present.

[0461] FIG. 64 illustrates another network architecture including a system located in the manufacturing or distribution chain for the device that provides the device provisioning or partial

provisioning, and any pre-activation required for the device to later activate on the network in accordance with some embodiments. Device credential, software and settings server 6420 provides a link to the network functions that generate or provide device credentials, and/or associate device credentials with activation profiles or pre-activation profiles in the network equipment (e.g., the billing system 123, service controller device control system 6225, gateways 410, 420, base station 125, credential generation and association server 6410, activation server 160, service download control server 1660 and/or other network apparatus). For example, the link between the device credential, software and settings server 6420 to the central provider core network equipment can be over the Internet 120 (e.g., a secure link over the Internet) as shown or over another connection such as a leased line. The device credential, software and settings server 6420 obtains credentials or partial credentials from the network apparatus that generates them, illustrated by the credential generation & association server 6410. Credential generation & association server 6410 need not be directly connected to the central provider core network 110 as shown, but can be located elsewhere (e.g., in another location connected by a secure Internet link). Credential generation & association server 6410 assigns credentials, or partial credentials, for use by device credential, software and settings server 6420. When these credentials are assigned to a device, they are programmed, loaded or otherwise associated with the device by device credential provisioning apparatus 6430, which is connected to the device wirelessly or via a wire line connection.

[0462] In some embodiments, a device software loading and programming apparatus 6440 provides software loading or device settings functions that form a portion or all of the provisioning or pre-provisioning device configuration, or form a portion or all of the device activation profile configuration, or form the device service owner, master agent or VSP device assignment or signature, and in some embodiments, using an activation tracking service (ATS) system. As discussed herein, the ATS monitors network connections and aspects of traffic that provide insight into which networks the device 100 is gaining access to, in some embodiments, for the purpose of ensuring that an OEM, master agent, device service owner or VSP is being compensated for devices that activate on a service provider network. In some embodiments, the ATS agent connects to a server counterpart that records and, in some embodiments, also analyzes the service or network connection information to make a determination of the type of access service the device is receiving and, in some cases, determine which networks the device is

activated on. In some embodiments, the ATS is installed on the device in a manner that makes it difficult to tamper with or remove so that the entity that is intended to get credit for device service activation does get credit (e.g., the ATS agent can be loaded into secure memory, it can be installed with software that makes it difficult to de-install, it can be installed on the modem possibly in secure memory, it can be installed in the BIOS, it can be installed deep in the OS kernel, it can be installed with one or more additional device agents that monitor the ATS agent and alert a network function or re-install it if tampered with). The SIM inventory 6450 is provided to illustrate that, in some embodiments, hardware elements (e.g., a SIM security module as shown) or hardware configurations are also installed or manipulated in device 100 and these operations and the recording of the resulting associations form a portion of the provisioning or pre-provisioning process.

[0463] In some embodiments, at the time the credentials or partial credentials are loaded, programmed, set, installed, read from the device or otherwise recorded, they are, in some cases, all associated together in a database that allows for later identification of the device and its appropriate provisioning and/or activation process through such associations. For example, this can involve reading device parameters such as MEID, MAC address, device type, or other information that is associated with the information being loaded or configured on the device. As discussed herein, this credential configuration and association information is stored in the network equipment responsible using it to configure the network to activate the device in one of the various embodiments disclosed herein.

[0464] Some embodiments include tying some or all of the activation provisioning steps and information settings together into a database that defines a higher level activation profile for a group of users(/devices), and a server is used to perform device and equipment programming for the devices in the group, including, for example, associating the following device information into the group definition: credentials, service owner or master agent, provisioning information and/or activation profile. Some embodiments further provide for this device group information being distributed to the various network equipment components required to activate the devices as discussed elsewhere. In some embodiments, this programming and device group association is accomplished using the VSP workstation server 4910. For example, a device can be

manufactured and distributed in a manner that provides flexible assignment of the device to a group that is assigned to an activation profile or a service owner.

[0465] In some embodiments, multiple activation servers 160 are provided (as shown), which illustrates that there can be multiple device activation servers 160 each with a different device activation experience and potentially controlled by a different VSP, service owner, service provider, OEM or master agent. As discussed herein, there are several ways that a device 100 can be routed to the proper activation server 160 so that the device provisioning and activation process can be completed. In some embodiments, all devices that are not activated are re-directed (or routed) to an activation server that reads one or more parameters in the device credentials. The device credential information can be determined either through the device identification information associated with the access network connection itself (e.g., MEID, IP address, phone number, security credentials, or other credentials identified for a device that gains access with the network), or with the aid of the device in a pre-arranged query-response sequence. The device can then be re-directed (or routed) to the appropriate activation server for that device, device group, device service owner or VSP. In some embodiments, the same process described above can be accomplished with a single re-direction from a service gateway 420 or 410, or another router enable network element. In some embodiments, the gateway or network element itself decodes the device credential information as described herein and performs the correct re-direct (or route) to the appropriate activation server 160 for that device. In some embodiments, the activation server 160 can be incorporated directly into the gateway 420 or 410, the base station 125 or other network component. In some embodiments, the activation server 160 can be incorporated into the service controller 122 or the service controller device control system 6225.

[0466] In some embodiments, apparatus other than the activation server are used to facilitate provisioning of credentials or partial credentials, or activation, during manufacturing or device distribution, and, for example, these apparatus can augment, supplement, compliment or replace the activation server function. Such apparatus include, for example, device programming equipment (e.g., device credential provisioning apparatus 6430, device software loading and programming apparatus 6440 or SIM inventory 6450), equipment that is networked into a central provider, MVNO or VSP database (e.g., device credential, software and settings server 6420) to

gain access to provisioning information or activation information that is programmed into a device or group of devices, or to place device credential or partial credential information in a network database for later recognition, or to receive or communicate security information such as certificates for devices or SIM modules that will later be used to complete provisioning or complete activation or gain access to a network. For example, these apparatus, or any other apparatus including the activation server, can be networked into a service provider network or device database, an MVNO network or device database or a VSP network or device database. In some embodiments, programming of the device credentials or other information associated with the service processor or device is provided, so that, for example, the device can be recognized by an activation server or similar network function at a later point in time so that provisioning or activation can be completed in an automated manner, potentially with reduced or no user involvement, that provides a provisioning or activation configuration that is in some way unique for the service provider or service provider partner, device type, user group, VSP, MVNO, master agent or other entity. In some embodiments, this programming is provided in a manner that is difficult to change without the proper authorization so that the device is properly associated with the proper “service owner” or master agent (e.g., for the purpose of activation incentive payments). For example, as discussed herein, various approaches can be applied to the device credential or other settings or software provisioning so that the settings or software are secure or protected, or so that if the software is removed, replaced or modified it is reported or replace or restored. In some embodiments, VSP control of the provisioning, partial provisioning or activation of devices is provided during manufacture or at different points in the distribution channel. As discussed herein, some of these embodiments allow the central provider to offer to service partners (e.g., VSPs, MVNOs, master agents, and/or OEMs) similar types of control for device activation experience design or device service assignment control (e.g., sometimes referred to as service provider device locking so that other service providers cannot provide primary access to the device) during the manufacturing or distribution process that are possible with devices manufactured and distributed for the central service provider.

[0467] In some embodiments, the device is provisioned before the user obtains the device with permanent credentials, temporary credentials or partial credentials. In this case, the necessary credential programming of the device occurs during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of

shipment. In some embodiments, provisioning of network information as discussed above is used, and the network information is provisioned at the same time, before or after the device information is provisioned. In some embodiments, the device provisioning information is programmed with dedicated apparatus that connects to the device either with wires or wirelessly. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or it can be partially or entirely networked into a database or provisioning solution located elsewhere and operated by the central provider, a VSP, OEM or other entity. For example, the apparatus to program the network portions of the provisioning information can also be networked and the operators who set up the required network programming for a device or group of devices may be in the vicinity of the servers that host the provisioning and management tools or they may network into the servers. In some embodiments, provisioning system operators have full or partial control of any device provisioning equipment associated with the entity they work for (e.g., OEM, VSP or master agent) but only have remote access via secure terminal, secure website or other techniques to network into a central provider or VSP server farm in which they control or partially control the network portion of provisioning capabilities for that subset of devices that are assigned to the entity they work for with (e.g. OEM, VSP or master agent).

[0468] In some embodiments, provisioning is accomplished over the air on the mobile access network for mobile devices, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment, such as a computer to perform the programming required to complete provisioning. In the cases in which the device is provisioned at point of sale or after point of sale, the device provisioning can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, in some embodiments, partial credentials that include information such as device type, OEM or service provider are used to assist in determining how to complete the provisioning, and the information can also include secure information, certificate or signature programmed into the partial credentials that is required for the network to perform the provisioning of the remaining credential information in the device and possibly the network. In some embodiments, any network information

used/required to provision the device or service is generated at the time the partial credentials are determined rather than beforehand.

[0469] In some embodiments, the device is activated for service before the user obtains the device with permanent credentials, temporary credentials or partial credentials, or with a permanent service account or a temporary service account. For example, in this case, the necessary steps of provisioning and activating service for the device can occur during manufacture, at some point in the device distribution, such as at a distribution depot or in a store, or at the point of sale or point of shipment. In some embodiments, the steps for activating service include one or more of the following: provision the device (e.g., with permanent, temporary or partial credentials), provision the necessary network databases and equipment to prepare them to recognize the device and associate it with the service profile and/or service plan, create or select the service account (e.g., permanent or temporary service account), select or create the service profile and/or service plan, program any elements in the device required to activate service (e.g., account ID, device aspects of the service profile and/or service plan), and program the necessary network databases and equipment with the required associations of device credentials and service profile and/or service plan policy settings. In some embodiments, the device oriented programming portions of the service activation steps occur at the same time, before or after the network oriented programming portions of the service activation steps.

[0470] In some embodiments, the device activation information is programmed with dedicated apparatus that connects to the device via a wireless or wire line connection. For example, the dedicated apparatus can be local to the location where the device is being provisioned, or the dedicated apparatus can be partially or entirely networked into a database or service activation solution located elsewhere and operated by the central provider, a VSP, OEM or other entity. For example, the apparatus to program the network portions of the activation information can also be networked and the operators who set up the required network programming for a device or group of devices can be in the vicinity of the servers that host the service activation and management tools or they can network into the servers. In some embodiments, activation server tools operators have full or partial control of any device activation apparatus associated with the entity they work for (e.g., OEM, VSP or master agent) but only have remote and partial access via secure terminal, secure website or other techniques to

network into the network portion of the activation tools that are controlled by the central provider or VSP. The server tools operators can be restricted in some embodiments to providing network activation information or settings only for those devices or device groups that are assigned to the entity they work for with (e.g., OEM, VSP or master agent). For example, the device control group restriction can be accomplished with a secure database that has secure sub-partitions for one or more entities so that they cannot impact the control of one another's network activation settings but can control their own devices. In this way, a centralized set of activation tools resources controlled by a central provider, VSP or other entity can be partitioned so that different entities can have partial or full control of the activation service definition for devices or groups of devices without impact or risk to others who share the network and activation tools resources.

[0471] In some embodiments, activation is accomplished with an over the air interface to a mobile device, or over the wired access network or WLAN connection for wired access networks, either before the user receives the device or after the user receives the device. In some cases, the device can be connected to general purpose equipment such as a computer to perform the programming required to complete activation. In the cases in which the device is activated at point of sale or after point of sale, the final device activation process can be triggered by a user initiated sequence, or can be initiated by an automated background sequence at any time after the device is powered on. In such cases, some embodiments call for a temporary service account that is used to bring the device onto the network before the user has input the information necessary to create a permanent service account. In some embodiments, a temporary or permanent service account can be applied to the device at the time the device reaches the network, and the type of account, service profile and/or service plan can be influenced (e.g., partially determined or informed) or determined by information embedded in the device credentials or partial credentials, such as device type, device ID, SIM, OEM or service provider. For example, the device credentials can also include secure information, certificate or signature that can be required by the network to perform the activation steps for temporary or permanent service account status. In some embodiments, in which the device is activated in this manner before the user information is available, or before the user has selected a pay for service plan, the service profile and service plan are set up for ambient services as described herein.

[0472] In some embodiments, the device is activated during the manufacturing or distribution process, and then the activated device status is suspended. Once the temporary or permanent service account is set up, with appropriate service profile and/or service plan and temporary or permanent credentials, in some networks and billing systems the service can often be more easily resumed once suspended as compared to provisioning and activating the device from scratch. The device is then later resumed (or re-activated) when some event triggers the resume process, such as when it ships to the end user or when the end user attempts to use it. This process prevents the network from needing to manage credentials and accounts for devices that have been activated but are not yet on the network.

[0473] In some embodiments, provisioning is accomplished at least in part with temporary credentials in a manner which is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary credential elements replaced at a later point in time by permanent credential elements in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary credential set is pre-programmed into the device along with a temporary or permanent service account including service profile during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming is performed for the network via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, a subset of the temporary credentials is recycled once it is replaced, if a temporary service account is not activated or used after some period of time, if a permanent account is not activated or used after some period of time, or if the credentials subset is revoked from the device for some other reason.

[0474] In some embodiments, more than one device is assigned one or more elements of the temporary credentials, such as the phone number, which may be limited in supply. In some embodiments, a network will accept more than one set of temporary credentials, one or more redundant elements, for two or more different devices. In some embodiments, a device that has two or more temporary credential sets, in which at least a subset of the credential elements are different for the sets, so that if one set of credentials has elements that are already being used to

access the network, then one or more reserve sets can be drawn upon to gain access to the network.

[0475] In some embodiments, the temporary credentials are used to log onto the network to conduct an over the air or over the network activation process in which an activation server reads at least a portion the device credentials to determine some aspect of how the device service profile. In some embodiments, the aforementioned over the air activation process is accomplished in the background without user intervention. In some embodiments, the over the air activation process is initiated when the user first attempts to use the device or when the user first attempts to access the network or upon user request or approval. In some embodiments, the over the air activation process is initiated using a temporary service account for the device and/or network to gain access to the network. In some embodiments, the over the air activation process is initiated after the user has entered the information required to create a permanent user account into the device or into the network. In some embodiments, the user is required to enter the aforementioned user information before using the device or using some aspect of the device. In some embodiments, the temporary service account is replaced by a permanent service account some time after the user has entered the necessary information to create a permanent account into the device or network. In some embodiments, the over the air activation process is initiated using a permanent service account assignment for the device and/or network to gain access to the network.

[0476] In some embodiments, the service profile is assigned to the device and/or network during the aforementioned over the air activation to be a pay for service profile with a free trial period. In some embodiments, the service profile assigned to the device and/or network during the aforementioned over the air activation includes pre-pay, post-pay, session based pay or pay as you go options for service. As will be apparent to one of ordinary skill in the art, various embodiments disclosed herein are particularly well suited for control or pre-pay services. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned over the air activation is an ambient service profile providing service access before all the user information is available to assign a permanent account. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing a service upgrade selection

option interface to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing transaction services to the user. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing bill by account functionality for the network. In some embodiments, the service profile that is assigned to the device and/or network during the aforementioned activation is an ambient service profile providing some amount of free networking or information service to entice the user to use the other ambient services. In some embodiments, the aforementioned ambient service is at least partially implemented with device based service activity control or control assistance. In some embodiments, the aforementioned ambient service is at least partially implemented by gateways, routers or switches in the network that are programmed according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account.

[0477] In some embodiments, activation is accomplished at least in part with a temporary service account in a manner that is automated and convenient for the user or device owner. In some embodiments, at least some subset of the temporary service account is replaced at a later point in time by permanent service account subset in a manner that is also automated and convenient for the user or device owner. In some embodiments, the temporary service account settings (e.g., including the service profile settings and/or the service plan settings) are pre-programmed into the device along with a temporary or permanent credentials set during the manufacturing or distribution process so that the device is activated with temporary credentials when it ships. In some embodiments, the aforementioned pre-programming for the network is performed via a secure set of server access equipment that networks into the network databases used to define the service profile and/or the service plan. In some embodiments, the device is suspended once it is activated but before the user is using it, and then resumed before or commensurate with the point in time that the user begins to use it. In some embodiments, some subset of the temporary service account is recycled once it is replaced, if the temporary service account is not used after some period of time, if the temporary service account is not upgraded to a permanent service account after some period of time, or if the activation is revoked from the device for some other reason. In some embodiments, more than one device is assigned to the

same temporary service account. In some embodiments, a network accepts more than one device on the same temporary service account. In some embodiments, a device includes or is associated with two or more temporary service accounts, in which at least a subset of the temporary service account elements are different, so that if one account is already being used to access the network then one or more reserve accounts can be drawn upon to gain access to the network. In some embodiments, the temporary service account is associated with a temporary credentials set. In some embodiments, the temporary service account is associated with a permanent credentials set.

[0478] In some embodiments, un-activated devices are detected by the network routing equipment (e.g., service gateways or routers in hierarchical networks or base stations with embedded gateways in flat networks) and the device routing is programmed to re-direct un-activated devices to an activation server network destination. For example, the activation server can first inspect the information associated with the device to determine if the device belongs to the list of devices, device types or device groups that the network is programmed to provide access to. For example, the information used to determine this can include device type, service provider, phone number, device ID, SIM ID or configuration, secure information used to qualify the device, IP address, MAC address, user, user group, VSP, OEM, device distributor, service distributor (master agent), service processor presence or configuration, presence or configuration of other software or hardware. There can also be some activation definition information embedded in the credentials, or associated with some portion of the credentials, or programmed additionally on the device that informs the activation server as to the service profile and/or service plan and/or service account that should be established for the device. If activation information (the service profile, service plan and/or service account information) is found through association with the device credentials (e.g., device ID, phone number, IP address, MAC address, SIM or other security credentials) rather than being read directly from information embedded in the device or device credentials, then the pertinent aspects of the credentials can be used as a cross reference to look up the service plan and/or service profile information stored in a database networked to or within the activation server. The activation information can include information to define a wide variety of service plans and service profiles that when properly implemented on the network functions, and perhaps device if necessary, can provide for a wide range of service activity policies, service billing policies, transaction billing policies and service account types that can be associated with the device over the air or over the network.

[0479] In some embodiments, once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server initiates the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up may be permanent or temporary. In some embodiments, the activation process described above is completed perhaps before the user has entered some or all of the user information necessary to set up a permanent service account, and, in these cases, a temporary service account can be set up. In some cases, the activation process can be completed in the background before the user has completed an attempt to access the network and the service profile can be set up to provide ambient services to a temporary service account. In some embodiments, the user is required to enter the information required to establish a permanent service account prior to gaining full use of the device, either on the device, on a computer or in the store, so that by the time the user begins using the device the above activation embodiments can provide for ambient services activation with permanent account status so that the user can purchase a service upgrade or any transaction without entering any more account information.

[0480] In some embodiments, a device status is changed from a temporary service account to a permanent service account. If the device is activated with a temporary service account, and the user information is available to set up a permanent account, then if the billing system rules and interfaces allow for such, the user information can be changed from the mock information to the actual user information while maintaining the same account identifiers in the billing system. If the billing system will not allow for such, then the user information can be used to establish a new account, the device credentials can be re-associated with the new account, in some cases, after modifying one or more of the device credential parameters, and the network functions can be re-programmed as required, and, in some cases, the device can be re-programmed as required to accommodate the new permanent account.

[0481] In some embodiments, code on the device pulls a temporary or permanent set of credentials. When the credentials are pulled, the network associates the device with an ambient service profile according to one or more of the following: embedded device information identifying device type, service owner (e.g., VSP), user group, or user, or device ID is cross referenced to a database that is populated some time from manufacturing time to post sale where the database provides information identifying device type, service owner (e.g., VSP), user group, or user. The device is then re-directed accordingly (e.g., for device based this is a matter of setting the policies or loading the software for the service processor, for the network based approach this is a matter of populating the routing tables and service profile). For example, credentials can be re-cycled after a period of time, and/or some portion of the credentials can be redundant with other devices. For example, this is essentially a dynamic service for (temporarily) assigning device credentials, and the duration of the temporary credential validity for that device ID can be time limited to give the user time to activate a real account or a free trial, session limited, or a longer duration of time that is perhaps refreshed each time the device logs on. For example, the device could also already have permanent or temporary credentials but not have a service account. The above process can be used to assign a temporary or permanent service account as well. Once the service account is assigned and the appropriate service profile is propagated to the network elements, the device can then be directed to or use the appropriate activation profile service activities or the appropriate ambient service activities.

[0482] In some embodiments, the device is activated in the background in a manner that is virtually transparent to the user. For example, at some point in the distribution channel, the device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device connects to the network and the gateways or routers re-direct the device to an activation server, as discussed above. As also described herein, the activation server either derives information from the device that informs the server what service the device should be activated with, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the activation server has determined the activation information from the device or from a look up based on some aspect of the device credentials, then the activation server causes all the necessary network settings and billing database entries to be

configured/programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. In some embodiments, the activation server can then also send the any necessary service profile and/or service plan settings required for the device to a provisioning and activation support software function on the device, such as various embodiments of the service processor, so that the device provisioning and activation can be completed. For example, the provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

[0483] In some embodiments, background activation is performed using the aforementioned activate/suspend process. At some point in the distribution channel, the device is programmed to seek to resume service as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. When the pre-programmed event is triggered, the device attempts to connect to the network and the gateways or routers re-direct the device to an activation server as described herein. As also described herein, the activation server either derives information from the device that informs the server that the device is ready to resume service, or the server derives that information from a database look up with a portion of the device credentials as the cross reference parameter. Once the server is aware of this information, it sends a message to resume service to the billing system, or other network function that controls the suspend/resume function, and the service is resumed.

[0484] In some embodiments, background activation is performed as described below. The service processor and the credentials are pre-programmed during the manufacturing or distribution process to provide the desired service profile support and/or billing profile support for the desired initial ambient service. As described herein, this programming can be accomplished with dedicated apparatus at the manufacturer or distribution depot. Furthermore, the party responsible for defining the service (e.g., typically the central provider, OEM, VSP, distributor or master agent) can network into the service processor programming apparatus to control service processor and/or credential programming for all or a subset or group of the devices or device types locally available. The service processor enabled device is programmed to seek the activation server system described above as soon as it is turned on, or as soon as some other event occurs like the user using the device or the user attempting to gain access. In some

embodiments, the activation server is the access control server previously discussed or the access control server can act in concert with another server that performs the activation function. When the pre-programmed event is triggered, the device connects to the network and the gateways or routers re-direct the device to the activation server. As also described herein, the activation server can communicate with the service processor to verify the service processor security credentials, agents and configuration.

[0485] In some embodiments, if the activation server determines that the pre-programmed settings stored in the service processor need to be modified to provide the latest version of the desired service, or if the service processor agent software needs to be updated, then this can be accomplished prior to completing the activation process. Once the service processor configuration and settings are confirmed, the activation server causes the necessary network settings and billing database entries to be programmed by sending the service profile instructions to the network provisioning and activation apparatus and the service plan instructions to the billing system. Given that the service processor can perform some or much of the service activity control or control assistance, the service control options are generally larger than without the service processor, and there can be less configuration to perform for other networking equipment to complete the provisioning and activation process. The provisioning can be with permanent credentials or temporary credentials, and the service account that is set up can be permanent or temporary.

[0486] In some embodiments, pre-programming and pre-activation of devices with temporary credentials and a temporary service account are used to ship devices that are pre-activated. Given that the credentials are temporary and can be recycled when the permanent credentials are assigned, concerns about using up too many pre-assigned credentials are reduced. In embodiments in which a portion of credentials elements can be used for multiple devices, this concern is further reduced. If there is a concern about too many activated devices being assigned that are not actually active and generating service revenue, then the suspend/resume process discussed herein can be employed. In some embodiments, the temporary credentials and/or temporary account can be replaced with permanent credentials and/or account assignments at any time as follows. When a pre-programmed event in the device is triggered, then the device initiates a program that seeks the aforementioned activation server or another server that has the

capability of fulfilling the device request to exchange the temporary credentials for permanent credentials and/or exchange the temporary account for a permanent account. The event that triggers the credential exchange can be the same or different than the event that triggers the service account exchange. The service account exchange can typically be triggered by the point in time that the user enters account information.

[0487] In some embodiments, the aforementioned ambient service is partly implemented with a combination of the techniques for pre-provisioning during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy provisioning capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are pre-programmed as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the provisioning credential elements are not all pre-programmed before the device ships, but a subset of the credential elements are programmed using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service activity control settings for the gateways, routers or switches that will result in the desired ambient services activity controls.

[0488] In some embodiments, the aforementioned ambient service is implemented with a combination of the techniques for pre-activation during manufacturing or distribution and at least partially implementing the service activity control (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage) required for implementing ambient using the service policy control capabilities in the data path gateways, routers or switches in the network. The gateways, router or switches are programmed to recognize the pre-activated device credentials as discussed herein according to the ambient access profile for the device to implement the ambient policies for network access control, routing control, traffic control or service monitoring and reporting for bill by account. In some embodiments, the device activation profile and/or service account are not pre-programmed in the network and/or the device before the device ships but the activation profile and/or service account are programmed

using the activation server technique discussed herein. This over the air automated provisioning is combined with the activation server reading the device credentials to derive the service profile activity control settings for the gateways, routers or switches that results in the desired ambient services activity controls.

[0489] In some embodiment, a VSP capability is enabled by providing a secure network connection to the service policy settings tools that define the device pre-provisioning settings, the device pre-activation service profile settings, the network equipment service activity control policy settings (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage), and the network billing system database. By providing server tools that enable all these settings to be controlled (or perhaps only observed in the case of the billing system) by a secure workstation or secure website interface that networks into the equipment that programs the settings, and providing for a secure partitioning of the devices that can be controlled by a given secure workstation or secure website interface, a central provider can provide VSP services to multiple entities who all have different device and service plan combinations that they desire different flavors of ambient services for. These techniques can also be extended beyond ambient to any device/service profile/service plan combo the VSP desires to create. In some embodiments, the networking equipment is implemented to secure device service group domains in which the service policies for a group of devices can be controlled. In some embodiments, the pre-provisioning and pre-activation techniques are substituted with the over the air activation server techniques discussed herein, and a secure device group partition capability is provided in the activation server as well so that the activation server device group partition control capabilities can be added to the secure device group partition control capabilities of the network gateways, routers and/or switches, the device programming tools and the billing system to form a VSP partition solution for over the air activation of various device/service plan combinations. In some embodiments, the device groups are relatively small so that beta trials of arbitrarily large or small size can be designed and implemented by defining a service control group as described above, and after fine tuning and perfecting the beta trial settings the device group can be expanded to publish the automated provisioning and activation service settings to a larger user or device group for production services.

[0490] In some embodiments, device based service activity control assistance (e.g., based on the various service processor embodiments described herein) is combined with simplified provisioning techniques described herein so that service processor enabled devices can be shipped with pre-provisioned credentials (temporary or permanent) or can obtain credentials in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain credentials and provisioning apparatus described elsewhere provide various approaches for provisioning pre-provisioned service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various approaches for over the air or over the network simplified post-sale provisioning for service processor enabled devices. For example, these embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

[0491] In some embodiments, provisioning includes provisioning partial device credentials that include, for example, a secure certificate that is used to authorize full credential provisioning and/or activation by performing a process for a later look-up/validation of the full device credentials. For example, the look-up/validation of the full device credentials can be performed by a gateway, router or similar network device that re-directs to a provisioning server and/or activation server or other network components that either: (1) recognizes the partial credentials that serve as a reference to direct the device communication to a specific provisioning/activation server determined from the partial credentials; or (2) does not recognize the partial credentials, and directs the device communication to a less specific provisioning/activation server that is not necessarily associated with a reference to the partial credentials.

[0492] In some embodiments, if the partial device credentials (e.g., temporary or permanent credentials) are being used for provisioning, then the partial credentials are read (e.g., and/or other credentials can be looked up based on the partial credentials as described above). The device is authorized if the proper credentials and/or secure certificate is present. The device credential provisioning is then completed (e.g., using activation server commands or settings to a

device based software and/or hardware element), and the credentials are, in some cases, also communicated to the various network equipment elements.

[0493] In some embodiments, if the partial device credentials are being used for activation, then partial or full device credential provisioning is performed, such as described above. A service account (e.g., temporary or permanent service account) is created or looked up based on the partial device credentials (e.g., a user account associated with the device through embedded partial or full credentials or a look up process, or based on a dynamically created/assigned temporary account associated with the device through embedded partial or full credentials). An initial service profile and, in some cases, an initial service plan (e.g., service control policy settings including a billing profile) are determined from embedded information and/or using a look up process (e.g., based on the device type and/or partial or full device credentials). The device is then programmed to enable access with the service profile and plan, and, in some cases, the various network components/elements are programmed to enable the service profile and plan, and, in some cases, proper entries in the billing system are made or confirmed, and the device credentials are, thus, activated for service.

[0494] In some embodiments, the above described provisioning and/or activation processes are performed with the provisioning server(s) and/or activation server(s) in the background with reduced, minimal or no user input required, for example, after the device is sold to the user and the user turns on the device so that by the time the user attempts to access the service using the device, the provisioning and/or activation process is already completed.

[0495] In some embodiments, device based service activity control assistance (e.g., based on the service processor embodiments) is combined with simplified activation techniques described herein so that service processor enabled devices can be shipped with pre-activated accounts (temporary or permanent), or can obtain activated account status in an automated manner that is convenient and efficient for the user or device owner. In some embodiments, the service processor embodiments in combination with the manufacturing and supply chain activation and provisioning apparatus described elsewhere provide various approaches for pre-activated service processor enabled devices. In some embodiments, the service processor embodiments in combination with the activation server variants discussed above provide various

approaches for over the air or over the network simplified post-sale account activation for service processor enabled devices. These embodiments can also be used for ambient services given that as discussed herein the service processor has capability to implement service profile policies for deep control of ambient service activity control.

[0496] As discussed herein, in some embodiments for activation, the network AAA (or other network function) either recognizes one or more aspects of a pre-activated device credentials and routes the pre-activated device communication to an activation server that is appropriate for that device (routing information either derived through look up of the credential aspect or by obtaining the required information directly from the credential itself), or the AAA (or other network function) does not recognize the credentials and routes the device communication to an activation server for unrecognized device credentials. In either case, in some embodiments, one or more of the credential aspects can then be used to perform a secondary determination of what provisioning and/or activation sequence to perform in association with the device, or which activation server sequence the device should be directed to. For example, one or more device credential aspects can be read and used as a cross-reference to determine a routing for the device communication (or the information required for routing can be in the device credential information itself) so that the device can be routed to the appropriate activation server sequence.

[0497] In some embodiments, an activation server sequence can be determined at least in part by using a browser server or a portal (e.g., http server, https server, WAP server or another standard or custom protocol server for a browser, embedded or automated browser or a portal client in the device). In some embodiments, the browser server is an http or https server. The pre-activated device communication can be routed to the https server in a manner similar to that described above, and the server can read the information embedded in the https communication to determine the device credential information required to initiate the correct provisioning completion and/or activation sequences. For example, the https header information, tokens, cookies or other secure information communicated over https from a secure embedded client on the device (or user) can either provide the activation server with the information required to perform the cross-reference to an appropriate provisioning and/or activation sequence, or the https embedded information or the embedded client (or user) information can instruct the

activation server on which services the device is to be provisioned and/or activated on and any necessary device or user information (e.g., device owner and/or billing information) can be exchanged, or the device might be provisioned and/or activated first on a free ambient service with temporary or permanent credentials or account.

[0498] In some embodiments, the service processor can be combined with the pre-provisioning and pre-activation techniques described above to create an ambient service solution that will work on roaming networks in which the central provider or VSP has no control or minimal control over the network elements. For example, the device includes a service processor pre-programmed for ambient service activity control as discussed herein, and the device credentials and other settings are pre-provisioned and pre-activated for the central provider network, all of which is described in numerous embodiments disclosed herein. Provided that the service provider has a roaming agreement with other service providers, or provided that the device may gain access to the roaming network, when the device is roaming it will be capable of ambient connectivity with bill by account functionality and all the other features of ambient. Furthermore, as also discussed herein, the ambient service activity control policies can be different for different roaming networks to accommodate the varying network costs and performance. Also, for example, it would be permissible to sign up for initial services or additional upgrade services with the central provider while roaming on the roaming partner network. One of ordinary skill in the art will appreciate that this also allows for creating a VSP or MVNO for the purpose of creating a clearing house for central provider service activations according to geography or user choice. By using a global multi-mode modem module, and maintaining service agreements with a multitude of carriers, the MVNO or VSP can provide consistent ambient services across multiple carriers and multiple geographies while still maintaining a good degree of cost control. Using bill by account capabilities, it is also possible to have an activation agreement where a roaming service provider agrees to refund the cost of ambient roaming. From the ambient service platform, the VSP or MVNO can then provide service purchase options to the user based on the carrier networks available to the device, or the VSP or MVNO can broker the user off to any of the carriers by activating the device onto the carriers main central provider service.

[0499] Accordingly, these embodiments provide flexible capabilities for activating a device or group of devices with a broad range of service profiles and service plans by simply programming the device with the proper credentials at some time during manufacturing or distribution, or simply programming a database associated with the network so that a portion of the device credentials can be used to look up the desired service profile and service plan. For example, various activation embodiments described herein are highly convenient for the end user and need not, in many cases, involve any human intervention.

[0500] The service processor 115, service controller 122, policy implementation and/or profile implementation and various embodiments disclosed herein are applicable to conventional communication products as well as machine to machine applications. For example, if the machine to machine device includes a service processor 115 with an activated account, then the service profile settings can be optimized for machine communications to provide only the limited access required to support the particular machine to machine application. This allows for cost optimized access services and prevents the machine to machine device or access modem from being misappropriated and used for some other service access than that intended. For example, by programming the machine to machine communications device at time of manufacture or during distribution with credentials or partial credentials that provide for automated provisioning and activation as described herein, the device can be automatically provisioned and activated on the service network with a service account when deployed, thus eliminating the need for costly or time consuming human intervention. The various embodiments that make it simpler to design, manufacture, test and deploy devices may also be equally applied to machine to machine devices. These embodiments include the service processor 115 developers kit and the automated provisioning and activation management tools among others. Also, the service analysis and test tools and the virtual service provider embodiments can also be applied to machine to machine applications.

Verifiable Device Assisted Services For Intermediate Networking Devices

[0501] It should be appreciated that the various service monitoring, notification, control and billing embodiments disclosed herein can also be applied to intermediate networking device applications.

[0502] In some embodiments, an intermediate networking device is a communications device in which the service processor 115 is configured at least in part to allow the intermediate networking device to act as a service intermediary or intermediate connection between the network and one or more end point devices (e.g., communications devices). In addition, a service controller 122 or other suitable network functions can be employed to assist with the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein. In some embodiments, an intermediate networking device does this by implementing the service policies required for assisting service usage control of the intermediate networking device and connecting the network to provide services to one or more end point devices that are connected to the intermediate networking device. In some embodiments, the intermediate networking device also monitors the service use activities of the intermediate networking device and/or the end point devices connected to the intermediate networking device. In some embodiments, the intermediate networking device and/or end point device service usage is verified to ensure that the service usage is within the expected ranges for the policies that are implemented. In some embodiments, the intermediate networking device connects with the network using one modem technology and connects with the end point devices using one or more additional technologies. In some embodiments, an intermediate networking device connects the end point devices to the network by passing, bridging, forwarding, routing, traffic shaping or otherwise allowing the end point devices to communicate with the network. Example intermediate networking device embodiments include a Wi-Fi to WWAN (e.g., 2G, 3G, 4G or other wireless wide area networking access technology) bridge or router device, a Wi-Fi to DSL, cable or fiber gateway device, a WWAN to DSL or Cable femto cell device, a WWAN and Wi-Fi to DSL, Cable or fiber back-hauled femto cell device, a WWAN to WWAN router device, a WWAN to WLAN, WPAN or LAN bridge, router or gateway device, or a WWAN back up connection device for an enterprise router.

[0503] An intermediate networking device can also be provided in some embodiments by including a bridging, forwarding or routing function between two modems in a communications enabled device that connects to the network. For example, an intermediate networking device configuration can be a cell phone, smart phone, mobile internet device or any other mobile device that includes a WWAN modem and a Wi-Fi, WLAN, WPAN or LAN connection that can be used to connect to other end point devices. For example, the mobile device WWAN modem

can connect to the network, a service processor 115 can be included on the device processor to assist monitoring, controlling and billing for services between the WWAN network and end point devices connected to a Wi-Fi modem. In addition, a service controller 122 or other suitable network functions can be employed to assist with verifiable service usage monitoring, control and verification as disclosed in numerous embodiments disclosed throughout herein. In some embodiments, the Wi-Fi modem can be configured in access point mode or in ad hoc mode to communicate with other end point devices in the area covered by the mobile device WLAN modem. In this manner, a service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein.

[0504] Another example embodiment is a notebook or sub-notebook computer with a WWAN modem and a Wi-Fi, Ethernet, Firewire, Bluetooth, near field or Zigbee modem in which the notebook processor has a service processor 115 running on the notebook processor and the service processor 115 is used to assist monitoring, control and billing for services communicated between the WWAN network and end point devices connected to the notebook or sub-notebook WLAN, LAN or WPAN. Another example embodiment is a Wi-Fi hot spot with a service processor 115 capability. Another example embodiment is a WWAN back up modem in an access network router where the back up modem connection to the WWAN network is used when the main wired network connection goes down, and a router processor or a WWAN back up modem processor runs a service processor 115 to assist monitoring, controlling and billing for services between the WWAN network and the access router (e.g., the service provider may only wish to enable a connection when the main wired network is down to ensure that the WWAN modem is not used for everyday access). In this manner, a service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments described herein.

[0505] Another example embodiment is a two-way home gateway configured to perform various functions such as reading power consumption of the home and/or components in the home, providing WLAN, WPAN or LAN connectivity for such components or to the power meters/controllers attached to such components, providing a WWAN or WAN connection to a

network that reads, records, monitors and/or controls the home and/or component power consumption, and possibly to provide other wide area network services for other devices in the home such as computers or entertainment electronics in a similar manner to the WWAN, DSL, cable and fiber gateway embodiments. The WLAN, WPAN connections can be made with one or more of Wi-Fi, Zigbee, Bluetooth, NFC or any other suitable wireless modem technology, and any desired wired LAN connections may be made with one or more of Ethernet, USB, Firewire, data over cable, data over power line or any other suitable wired modem technology. The WWAN connections can be made with one or more of 2G (e.g. CDMA 1xRT, GPRS), 3G (e.g. WCDMA UMTS/HSPA/non-MIMO HSPA+, CDMA EVDO/A/B, 802.16d/e WiMax), 4G (e.g. LTE, MIMO HSPA+, MIMO 802.16m WiMax) or any other suitable modem technologies and the wired WAN connections may be made with one or more of DSL, Cable, fiber or any other wired modem technology. A service processor 115 and a service controller 122 or other suitable network functions can be employed to enable the verifiable service usage monitoring, control and verification as disclosed in numerous embodiments disclosed throughout herein.

[0506] In some embodiments, an intermediate networking device can be used to connect one end point device to a network and assist in implementing service policies, or an intermediate networking device can connect multiple end point devices to one or more networks and assist in implementing service policies. In some embodiments, an intermediate networking device can be associated with one service profile, one service plan or one service account, or an intermediate networking device can be associated with multiple service profiles, multiple service plans or multiple service accounts. In some embodiments, end point devices connected to an intermediate networking device can have service usage policies implemented in aggregate for all end point devices, or service policies can be implemented differentially for different end point devices.

[0507] In some embodiments, an intermediate networking device can have a network connection associated with a single account and manage QOS between end point devices under one umbrella service profile or collection of profiles. In some embodiments, an intermediate networking device can treat all connected end point devices equally from a service sharing or QOS perspective so that, for example, service usage is based on end point device demand and/or contention. In some embodiments, an intermediate networking device differentiates service

QOS between different end point devices based on end point device service demand or service usage patterns, EDP device type or device group, end point device user or user group, end point device service account status or service plan status, or end point device application type, and/or traffic type or service type.

[0508] As discussed herein, the service processor 115 function assisting intermediate networking device implementation can be included on the intermediate networking device, can be included in part on the intermediate networking device and one or more end point devices, or can be implemented mainly or entirely on one or more end point devices.

[0509] In some embodiments, an intermediate networking device can be constructed in which end point devices connect to the intermediate networking device and gain access services to a WWAN network through a WWAN/Wi-Fi enabled intermediate networking device that is supplied with services associated with a single account and service profile. The intermediate networking device service processor 115 can assist in monitoring, control and billing for WWAN service usage for all end point devices in the area covered by the intermediate networking device Wi-Fi link. In some embodiments, end point devices receive service on first come first serve basis with no differentiation. In some embodiments, end point devices receive fair distribution of services so that if one end point device is using more significantly more service than the other end point devices, or is demanding more service than the intermediate networking device service profile settings provide for a single end point device (e.g., “bandwidth hogging”), then the high demand end point device is throttled and the other end point devices are not. In some embodiments, end point devices receive hierarchical distribution of services based on one or more of service type, device type, user type, and/or account status. In some embodiments, an intermediate networking device can provide for a large or unlimited number of end point devices to connect to the network and simply control aggregate service usage parameters for the intermediate networking device WWAN connection. In some embodiments, the intermediate networking device limits the number of end point devices that are allowed to connect to the WWAN network according the end point device count limits programmed in the service processor 115 service profile settings in the intermediate networking device. In some embodiments, end point device traffic can be identified by various end point device credential aspects including, for example, by Wi-Fi ID, MAC ID, IP address, user ID, LAN tag, end point

device agent credentials, and/or browser token or cookie. In some embodiments, the intermediate networking device service account can be billed for overall service usage and/or by number of end point device connections allowed or experienced. In some embodiments, as the intermediate networking device user or owner signs up for a higher end point device connection count, one or more aspects of the service usage policy implementation and/or profile implementations in the service processor 115 profile settings can be increased.

[0510] The various verification techniques described herein can also be applied to the intermediate networking device and extended to multiple end point devices. For example, network based service usage measures for verification can be applied to the intermediate networking device just as if the intermediate networking device were an end point device. For example, network based service usage measures (e.g., IPDR information) can be used to perform network verification checks to ensure that intermediate networking device service usage is within acceptable ranges based on intermediate networking device policy settings as similarly described with respect to various device embodiments. In some embodiments, in the event intermediate networking device service usage is outside the policy limits set for the intermediate networking device service processor 115, a notification can be sent to the intermediate networking device main account owner. The main intermediate networking device account owner can also be required to acknowledge the notification. The notification can also be sent to one or more other users of the intermediate networking device connection, including possibly all users. Other actions that can be taken if the network based intermediate networking device service usage measure does not match the policy limits set on the service processor 115 include notify the user, notify the user and require acknowledgement, bill the user for service overage, suspend the end point device, quarantine the end point device, SPAN the end point device, and/or alert network manager or alert an automated network troubleshooting function. In some embodiments, a device based usage measure can be verified against a network based service usage measure. It will now be apparent that the various service processor 115 verification embodiments, service controller 122 verification embodiments, network verification embodiments, authentication embodiments, and tamper prevention or detection embodiments, such as those shown in and described with respect to FIGS. 22A, 22B, 23, 26A-26H, 27A-27P and 28A-28E, can be applied to intermediate networking device applications and embodiments.

[0511] In some embodiments, it is desirable to match up individual end point device or user intermediate networking device service usage with other service usage measures. For example, the individual end point device service usage measures logged or reported from the end point devices and/or the intermediate networking device can be aggregated to form a total intermediate networking device usage measure that is compared to an aggregate intermediate networking device usage measure logged or reported in the network. In some embodiments, if these measures do not match, then an error condition results and an action is taken. In some embodiments, the aggregate intermediate networking device service usage measure is compared to the aggregate network based service usage measure and as long as these two measures are within an acceptable tolerance, then the intermediate networking device service usage measures are trusted and can be used for deeper intermediate networking device and end point device usage measures for service control and/or billing than may be possible in the network. In such embodiments, the individual end point device service usage measures gained from the intermediate networking device or end point device can be used to verify end point device service usage versus service policy allowances. In some embodiments, end point device service usage measures are compared with intermediate networking device measures for the same end point devices.

[0512] In some embodiments, the IPDR records for one or more networks can include individual end point device service usage information. This is the case for example when the IPDRs include information broken down by end point device credential, such as IP address or other end point device credential. In such cases, intermediate networking device embodiments can be employed in which the individual end point device service usage information measured in the network can be compared with the service usage policy allowances or limits for the end point device. Also, in some embodiments, the individual end point device service usage measures from an end point device service usage monitor and/or an intermediate networking device service usage monitor can be compared with the network based service usage information to verify an end point device and/or an intermediate networking device service usage monitor is operating properly.

[0513] As similarly described with respect to end point device embodiments with no intermediate networking device between the end point device and the network, in some

intermediate networking device embodiments, service usage and service usage monitor reports can be periodically verified by performing a SPAN function on the traffic for an intermediate networking device. The SPAN traffic can be analyzed in a real-time manner or in a non-real-time manner in the network and the results can be compared with the intermediate networking device or end point device service policies or service usage measures.

[0514] The synchronized device notification and acknowledgement embodiments can also be employed in the case in which one service account is applied to the intermediate networking device. The service usage counters in the intermediate networking device can be synchronized or updated with the network based measures and the differences between the two may be minimized. The service usage notification can be sent to one or more of the end point devices connected to the intermediate networking device. For example, the notification can be sent to the intermediate networking device manager or service owner, all end point devices or the most active end point devices.

[0515] Similarly, user preference feedback can be collected from one or more of the service users connected to the intermediate networking device. In some embodiments, user preferences or user service selections or service settings are collected from one user or a subset of end point devices used by the service subscriber. In some embodiments, more than one service user can provide preference information or service settings even if there is only one user account. In some embodiments, there are multiple service subscribers each providing preferences. In some embodiments, as similarly described with respect to various device embodiments, user preferences can be used set service control policies that provide the user with their selected balance of cost and service capability in a manner that meets network neutrality requirements. Similarly, in some embodiments, the service monitoring and customer resource management information collected on the intermediate networking device or end point devices can be filtered according to user privacy preferences to maintain the level of user privacy selected by the user.

[0516] Adaptive intermediate networking device policy implementation can also be performed in the intermediate networking device service processor 115 embodiments, as similarly described with respect to various device embodiments. In some embodiments, the

service policy implementation for the intermediate networking device can be adapted by the service processor 115 agents (e.g., policy control agent 1692 working to control the settings in policy implementation agent 1690, and/or another service processor agent or function) to achieve a higher level service usage goal. In some embodiments, the usage goals or adaptation can be based on aggregate end point device usage for the intermediate networking device network services, and in some embodiments, the higher level usage goals or adaptation can apply to one or more individual end point devices.

[0517] In some embodiments, even though there is one intermediate networking device account, there can be multiple options for multi-end point device or multi-user operation in which the number of end point devices, number of users or service capabilities for some of the end point devices or users are selectable. These parameters are accommodated by an intermediate networking device service profile that includes the service capabilities that are to be delivered to a multitude of end point devices or users. In some cases, some end point devices or users have a different profile within the intermediate networking device service processor 115 with differentiated capabilities as compared to the intermediate networking device service processor 115 profile for other end point devices or users. This is the case for some of the examples provided herein. These multi-end point device or multi-user service profiles in the intermediate networking device service processor 115 can share services equally or can allow more capable access services to some end point devices or users than others. In some embodiments, a service profile implemented by the intermediate networking device service processor 115 for one end point device or user is different than that in the service profile implemented by the service processor 115 for another end point device or user (e.g., providing differentiated service profile implementations by end point devices and/or users). End point devices can be uniquely identified for purposes involving implementation of different service profiles in the intermediate networking device service processor 115 agents (e.g., depending on the embodiment, service monitor agent 1696, policy implementation agent 1690, policy control agent 1692, application interface agent 1693 and/or other service processor agents or functions) based on a number of parameters, such as IP address, local area network address (e.g., Wi-Fi address), MAC address end point device ID, user ID, and/or end point device application layer tag. This allows for independent service usage monitoring and control for different end point devices or users.

[0518] In some embodiments, an intermediate networking device also bridges services to end point devices or users that have individually managed service profiles, service plans or service accounts. As discussed herein, individual end point device service policy implementation and/or service profile implementation can be accomplished by classifying end point device service usage according to an end point device identifier so that service monitoring, control assistance and reporting may be differentiated between one or more end point devices. These end point device identifiers can then be associated with a different service plan or account in the service processor 115 and/or billing system 123. The end point device or user specific service usage monitoring, reporting, notification and control assistance can be accomplished by running one or more profiles for each end point device or each user.

[0519] It will now be apparent that billing can also be implemented with a single account encompassing service usage for all users or end point devices connected to an intermediate networking device, or for individual users, end point devices, user groups or end point device groups connected to an intermediate networking device. As similarly described with respect to the service profile, this is accomplished by associating service usage events and associated billing events with an end point device identifier, user identifier, end point device group identifier, and/or user group identifier.

[0520] In some embodiments, end point devices or users connect to more than one intermediate networking device with the same service account, service plan or service profile. In some embodiments, the intermediate networking device requires an authentication sequence for the end point device or user before allowing connection to the network through the intermediate networking device. This authentication sequence can involve the end point device communicating an active account or admission credential with the intermediate networking device. The intermediate networking device can compare the credential with a local database or may query a database in the network to admit the end point device to the intermediate networking device network connection. In either case, provided the user credential or network authorization process is passed, the service processor 115 service profile settings for the end point device are applied and service is then established as discussed herein. In these cases, the verification can be accomplished as described herein. In some embodiments, even if the end point device does not have a service processor 115, provided that the intermediate networking

device service policy implementations and/or service profile implementations are verified as described herein, then the intermediate networking device will accurately assist in control and reporting of service usage for the different end point devices or users, and the appropriate service policy controls and/or billing can be maintained.

[0521] In some embodiments, when the end point device attempts connection to the intermediate networking device, if the user or end point device does not already have an active account or logon credential that the intermediate networking device recognizes, then the intermediate networking device can offer the end point device or user a service sign up experience. This experience can be implemented in a number of ways, including a website, WAP site, portal, download of agent software, and other methods. For example, an automated recognition of new devices can redirect unauthorized end point devices to browse into a website, WAP site, or portal site located on the intermediate networking device or in the network. If the site is located on the intermediate networking device, it can be cached and refreshed at a time of day when the network is not overly busy. Once on the site, the user or end point device selects the plan choice they desire, inputs account information and, in some embodiments, downloads device agent software to aid in network service policy implementation and/or profile implementation with the intermediate networking device. Once the user signs up, the information is logged into the network data base, the service account is established and the intermediate networking device service profile for that user or end point device is activated and the user can begin using the service.

[0522] In some embodiments, a website, WAP site, or portal site located in the intermediate networking device can be used to provide the end point device user with a service usage monitor interface and a service purchase interface for cases in which the end point device does not possess any special software to allow it to display a more specialized service usage monitor function for information received from the intermediate networking device or network service usage counters. The service usage monitor for the intermediate networking device can be synchronized, as similarly described with respect to various device embodiments. In some embodiments, the service usage notification system can also display cost data from a usage to cost look-up function. In some embodiments, the service usage notification system can display projected service usage or projected cost, as similarly described with respect to various device

embodiments. The service usage monitor to drive these service notification embodiments can be located on one or more of the end point device, the intermediate networking device or the network.

[0523] In some embodiments, if multiple accounts are serviced by one or more intermediate networking devices, verification can be performed on the service controls for the end point device or user service usage. As will now be apparent, just as with the intermediate networking device, the end point device or user service usage comparison with usage policy settings can be verified in the ways described herein. If the usage is found to be out of policy, then any of the out of policy actions described herein can be performed, including, for example, notify the end user, notify and require acknowledgement, bill for overage, suspend, quarantine, SPAN, and/or flag to network manager or network error handling function. For example, the verification methods shown in and described with respect to FIGS. 22A, 22B, 23, 26A-26H, 27A-27P and 28A-28E can be applied for the embodiments where intermediate networking devices have multiple account, multiple service plan, multiple service profile, multiple end point device, and/or multiple user capabilities.

[0524] It will be apparent that the various embodiments described herein for automated provisioning and activation also can similarly be applied to the intermediate networking device embodiments. It will also be apparent that the various virtual service provider embodiments can similarly be applied to the intermediate networking device embodiments.

[0525] Ambient services can be employed on the intermediate networking device and the ambient services can thus be provided to the end point devices. It will be apparent that the ambient service profile embodiments disclosed herein can similarly be applied to the intermediate networking device, and then the intermediate networking device can supply those ambient services to end point devices connected to the intermediate networking device. It will also be apparent that the intermediate networking device can provide an ambient service profile as described herein to end point devices or users that have not yet signed up for service, while providing other paid for service profiles to end point devices or users that have signed up for service.

[0526] Bill by account embodiments can similarly be applied to the intermediate networking device embodiments. For example, bill by account can be used in embodiments in which all end point devices or users are connected to the intermediate networking device under one account, or to embodiments in which some end point devices or users are accounted for separately with different service accounts, service plans or service profiles. In either case, it will be apparent that using one or more of the end point device or user identification credential aspects discussed herein can be used in a bill by account profile to account for any end point device or service activity. In such embodiments, billing event reports for those activities that include the end point device or user identifiers can also be provided for billing mediation and reconciliation down to the individual end point device or user level. For example, this allows for very deep service monitoring and billing capabilities with intermediate networking devices.

[0527] The intermediate networking device embodiments described above also have uses in machine to machine applications. It will be apparent that if the end point device includes the correct credentials to gain access to an existing account, or to allow an automated provisioning and activation account to be established, then the end point device can be connected to the network through the intermediate networking device without human intervention. Furthermore, the service profile that is established with the end point device for machine to machine communications can be set up to provide the access required to support the machine to machine application allowing for low cost access services and preventing the end point device from being misused for some service other than that intended. For example, the verification techniques and embodiments disclosed herein can similarly be applied to such machine to machine applications.

[0528] It will be apparent that the identifiers discussed above for bill by account mediation with accounting down to the individual end point device or user level can be combined with a billing mediation server in the network that accepts intermediate networking device billing events with end point device identification or user identification indexed billing, performs the necessary bill by account mediation functions, formats the billing events into the format used by the billing system, and transmits the mediated billing information to the billing system 123.

[0529] In some embodiments, the intermediate networking device service processor 115 functionality can be split. The division ranges from some or all of the service processor 115 on the device to some or all of the service processor 115 on the intermediate networking device.

[0530] In some embodiments, all of the service processor 115 is on the intermediate networking device. The end point device does not participate in service processor 115 functions and has no service processor 115 interface software. In some embodiments, the end point device has small subset of service processor 115 capabilities, including, for example, a service notification UI or a logon client with credentials. In some embodiments, service monitoring is implemented on the end point device or on both the end point device and in the intermediate networking device. In some embodiments, the end point device has additional service processor 115 capabilities including, for example, application layer tagging that associates application layer activity with service processor 115 service monitoring or service policy implementation and/or service profile implementation information. This can be accomplished by a range of techniques, for example, transmitting the application tagging information disclosed elsewhere to the intermediate networking device service processor 115 so that the policy implementation may be accomplished with knowledge of the application layer information. Another example involves assigning IP addresses in the intermediate networking device networking stack to the end point devices so that different types of end point device traffic can be routed into service processor 115 traffic shaping queues, each queue having a policy profile implementation engine, and application layer tagging information or similar traffic identifying information is used to determine which policy implementation engine the traffic should be routed to in order to accomplish the desired traffic shaping for the traffic type, application type, service type, and/or content type. In some embodiments, the traffic control policy is implemented on the end point device either with an application layer traffic controller, or by implementing more of the service processor 115 functionality, as similarly described with respect to various device embodiments. In the end point device service functionality example, most or all of the service processor 115 functionality is implemented on the end point device and the intermediate networking device functionality can be reduced to a bridging, forwarding or routing function between the end point devices and the network that performs little or no service control, monitoring and/or billing functions. For example, the service usage monitoring agents can also be provided on the end point device to aid in verification.

[0531] In embodiments in which the end point device requires agent software, the software can be loaded at time of manufacture or during distribution, loaded later, and/or made available for download through the intermediate networking device. In the case in which the end point device agent SW is downloaded through the end point device, there can be locally cached copies of the SW for one or more OS variants stored in a cache on the intermediate networking device, with the cache being updated over the network at convenient or conducive times, or the software can be downloaded live over the network when it is needed by the end point device. Logging the service usage to download this software is another example in which bill by account functionality can be used to track network traffic that may not be desirable to bill to an end point device owner or user, and bill by account functionality can be used to log and mediate such usage out of the user or end point device owner's bill.

[0532] Any end point device agent software required to connect to the intermediate networking device can also be implemented as a service processor 115 developer's kit as described herein and distributed to aid manufacturers, service provider and virtual service providers in bringing new devices onto networks with intermediate networking device capability.

[0533] In the case of a femto cell intermediate networking device, in some embodiments, it is desirable to facilitate handover from the WWAN network to the femto cell. In some embodiments, this provided in the intermediate networking device service processor 115 in a variety of ways. In some embodiments, the voice and data traffic is routed through a VPN tunnel controlled by the service processor 115 and connected to a network element, such as the transport gateway or another specified traffic concentration destination for the femto cell. In some embodiments, the voice traffic, the data traffic or both can be routed in secure or open Internet channels to different destinations, or the data can be routed directly to the Internet destination specified by the packets. In some embodiments, the femto cell intermediate networking device controls the femto cell frequencies or local frequency channel strength surveys over the intermediate networking device control channel. In some embodiments, the service processor 115 has a VPN connection to a network base station hand off controller to assist in handoff to and from the WWAN network and/or has the capability to instruct the end point device and the base station handoff controller. In some embodiment, whenever an end point device authenticated for femto cell access is within range of the femto cell, the service

provider desires to set up a service processor 115 profile to get the end point device to connect to the femto cell even if it has a strong signal with one or more WWAN base stations so that the WWAN traffic may be offloaded. In some embodiments, the service processor 115 can form a secure control plane link with network AAA functions to manage authorization and admission of end point devices the femto cell has not yet admitted, or the network policies can require re-authorization every time a end point device attempts access. Once an end point device is connected to the femto cell intermediate networking device, the verifiable traffic monitoring, control and billing functions described herein can be applied to various application embodiments. For example, the intermediate networking device service policy verification techniques disclosed herein, as similarly described with respect to various device embodiments, can similarly be applied to the femto cell intermediate networking device embodiments.

[0534] In some embodiments, the service provider desires to keep the number of end point devices or users that access an intermediate networking device below a certain count specified in the service processor 115 profile. In some embodiments, this is accomplished by controlling the number of IP addresses allowed onto the intermediate networking device local area side connection. In some embodiments, this is facilitated by observing the end point device identification parameters available in the end point device traffic. In some embodiments, this is facilitated by observing the traffic patterns to determine the likely number of devices connecting to the network. For example, traffic demand patterns can be examined to determine how many users are likely to be demanding access at one time. Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

INCORPORATION BY REFERENCE

[0535] This application incorporates by reference the following US applications:

[0536] Application No. 12/380,780 entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed March 2, 2009; provisional Application No. 61/206,354 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed January 28, 2009; provisional Application No. 61/206,944 entitled SERVICES POLICY COMMUNICATION

SYSTEM AND METHOD, filed February 4, 2009; provisional Application No. 61/207,393 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009; and provisional Application No. 61/207,739 entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 13, 2009.

WHAT IS CLAIMED IS:

1. A system, comprising:
 - a processor of a communications device configured to:
 - store a first set of device credentials for activating the communications device for a first service on a first network; and
 - send an access request to the first network, the access request including the first set of device credentials; and
 - a memory of the communications device coupled to the processor and configured to provide the processor with instructions.

ABSTRACT OF THE DISCLOSURE

Various embodiments are disclosed for a services policy communication system and method. In some embodiments, a communications device stores a set of device credentials for activating the communications device for a service on a network; and sends an access request to the network, the access request including the set of device credentials.

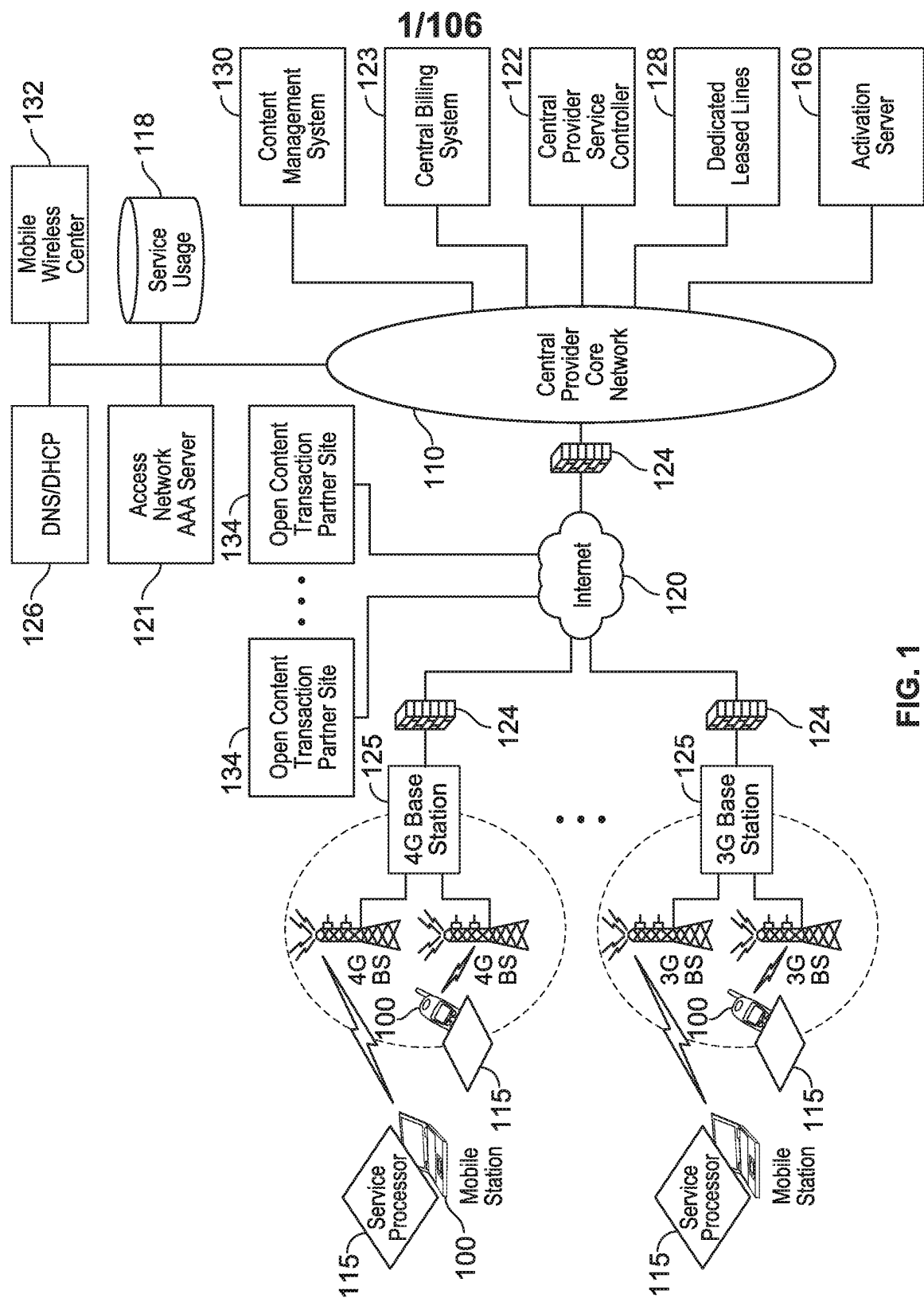


FIG. 1

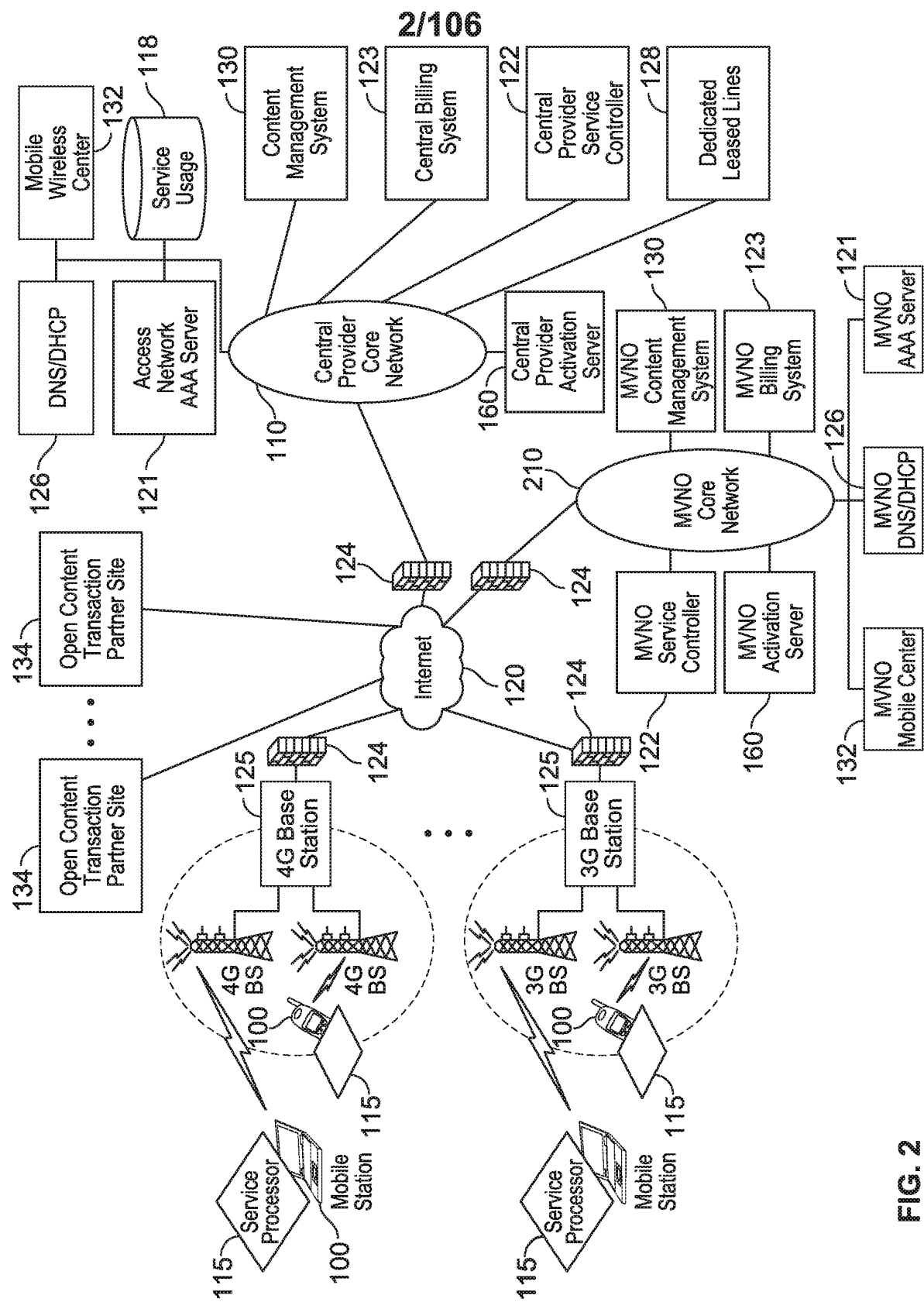


FIG. 2

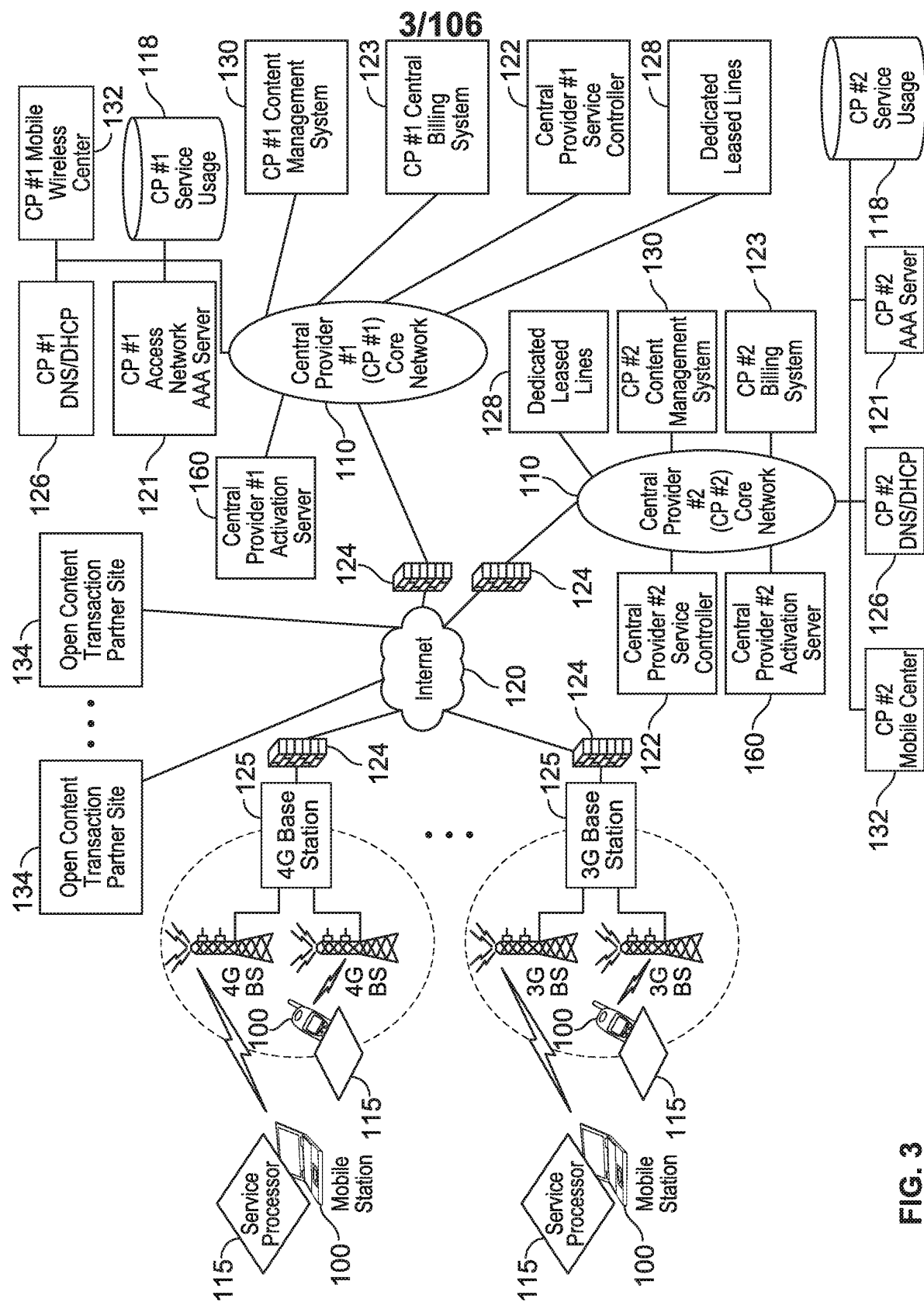


FIG. 3

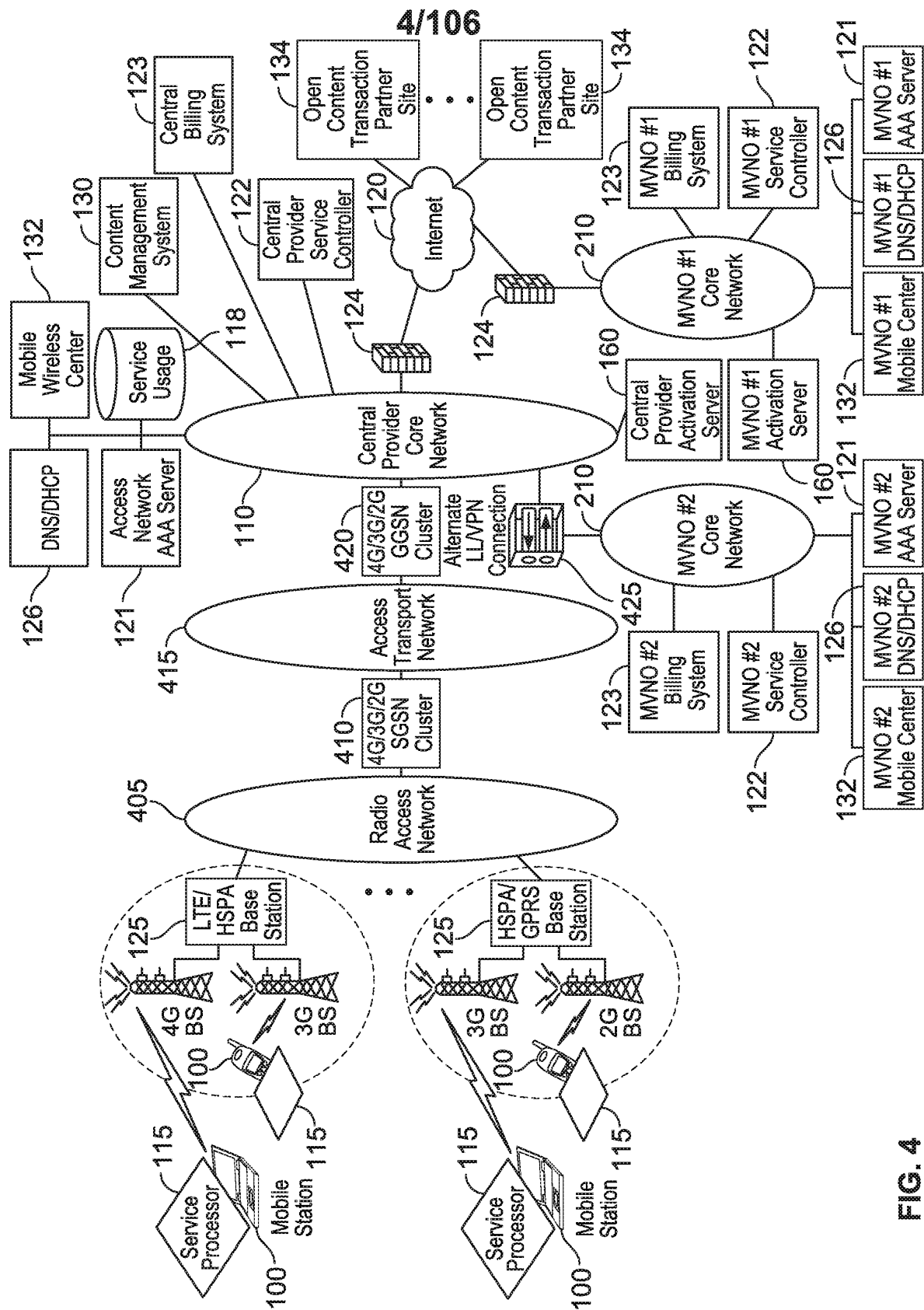


FIG. 4

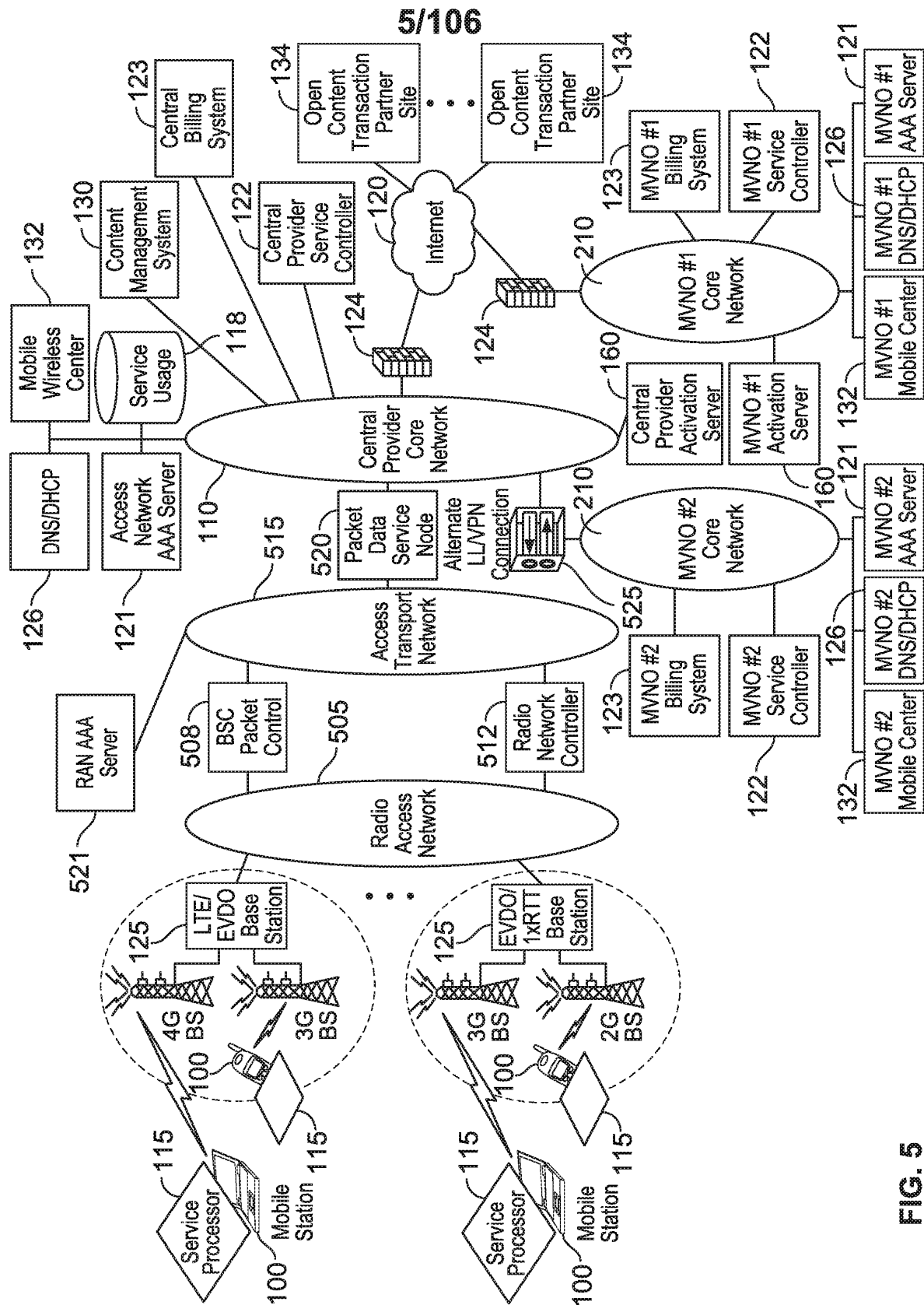


FIG. 5

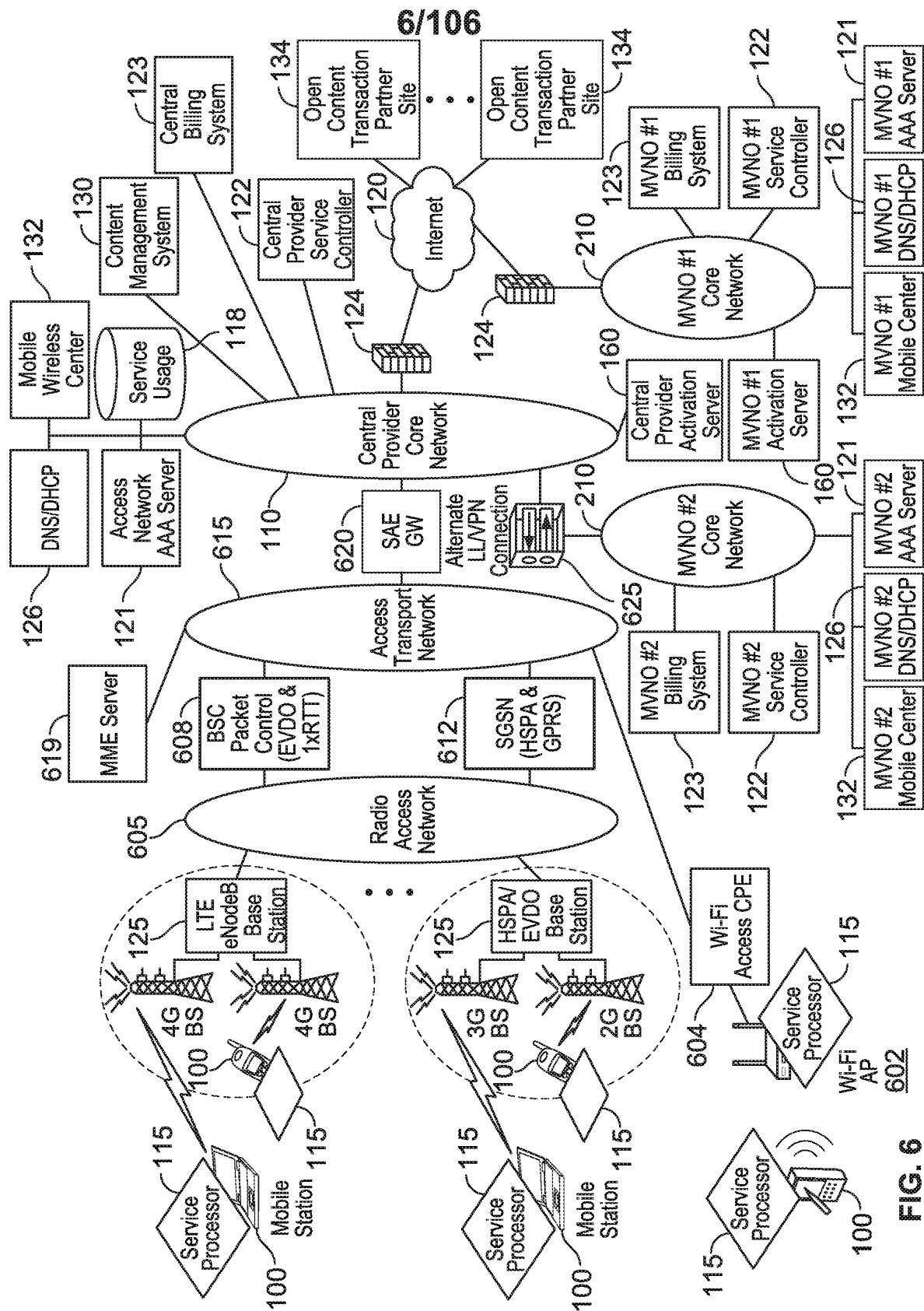
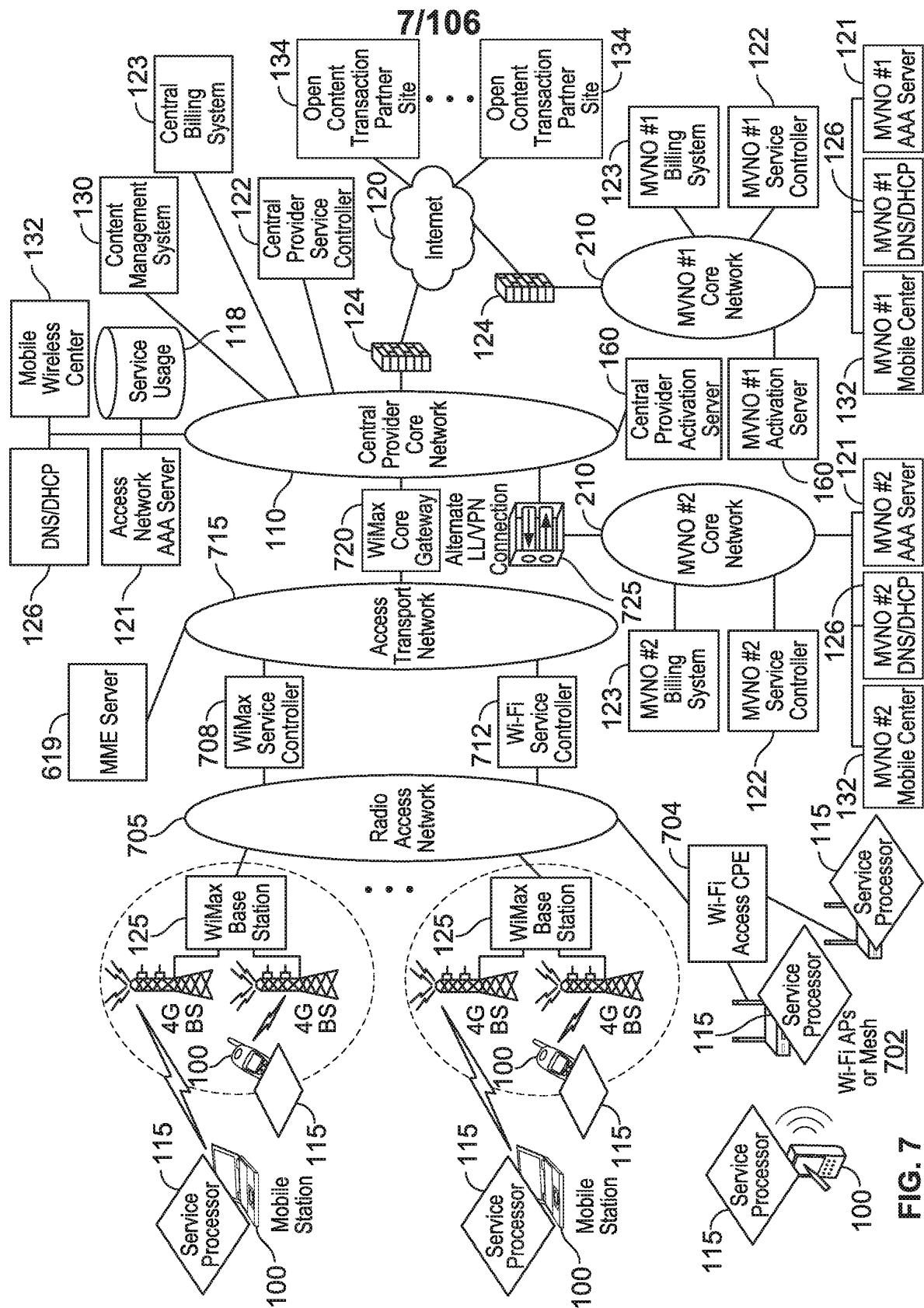


FIG. 6



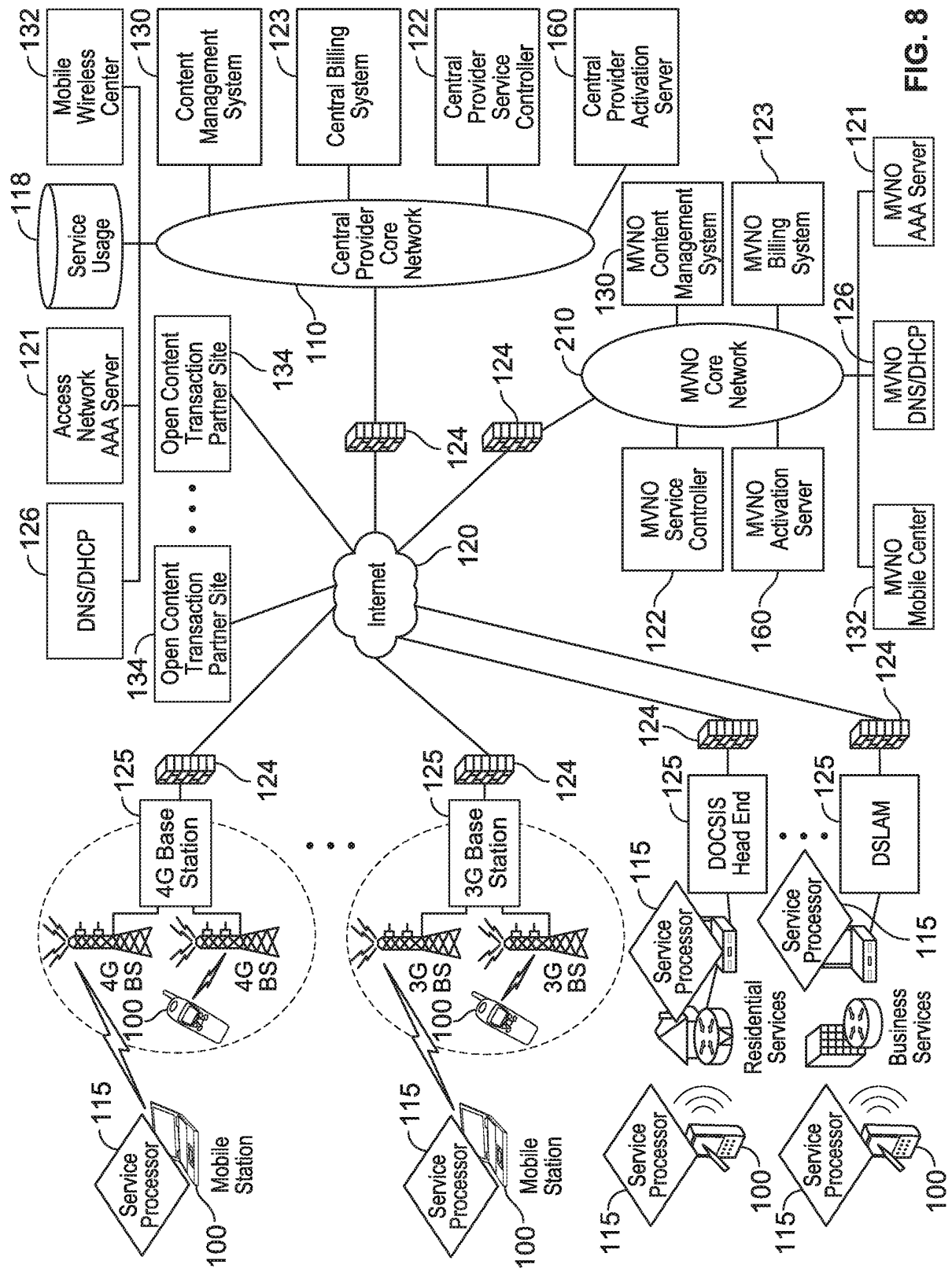


FIG. 8

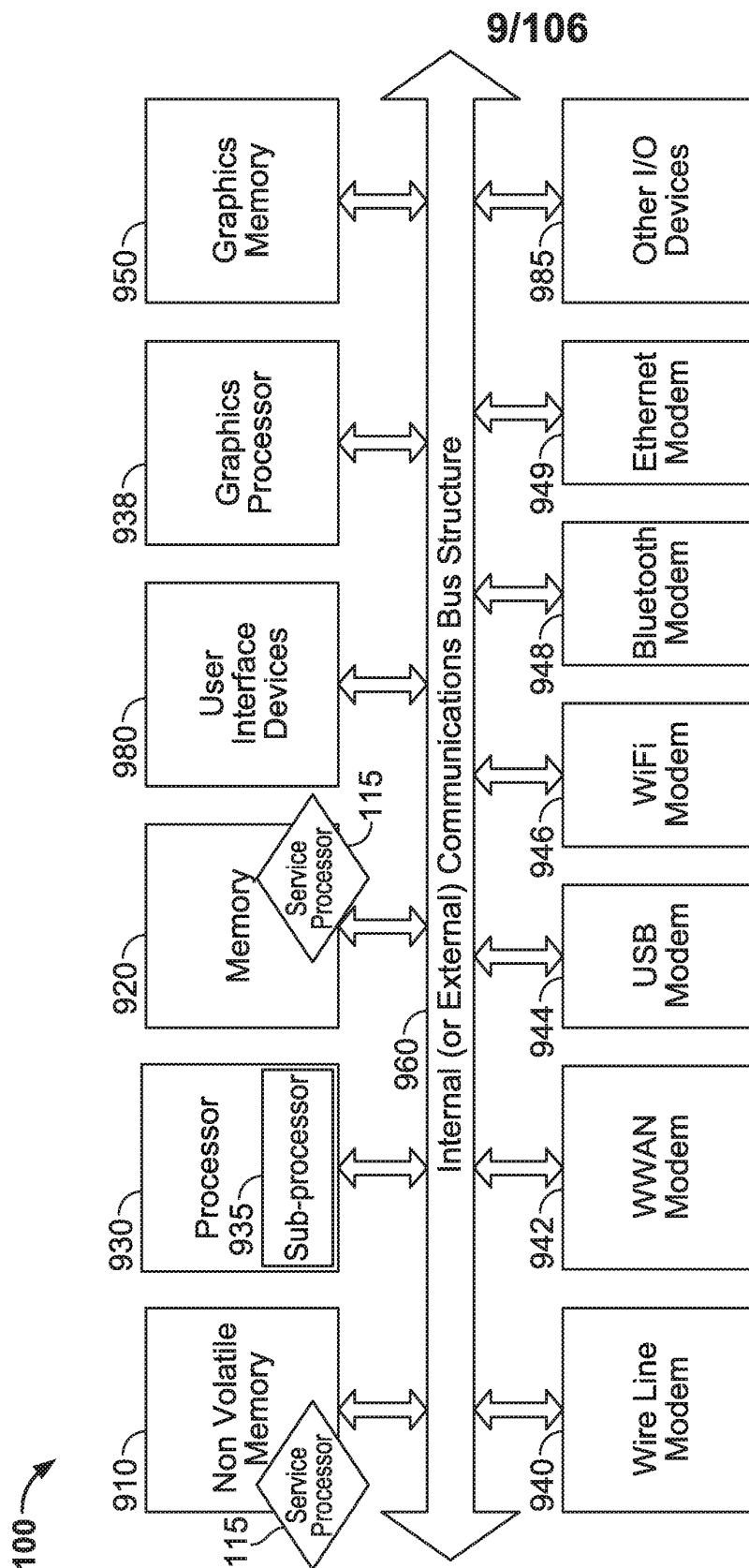


FIG. 9

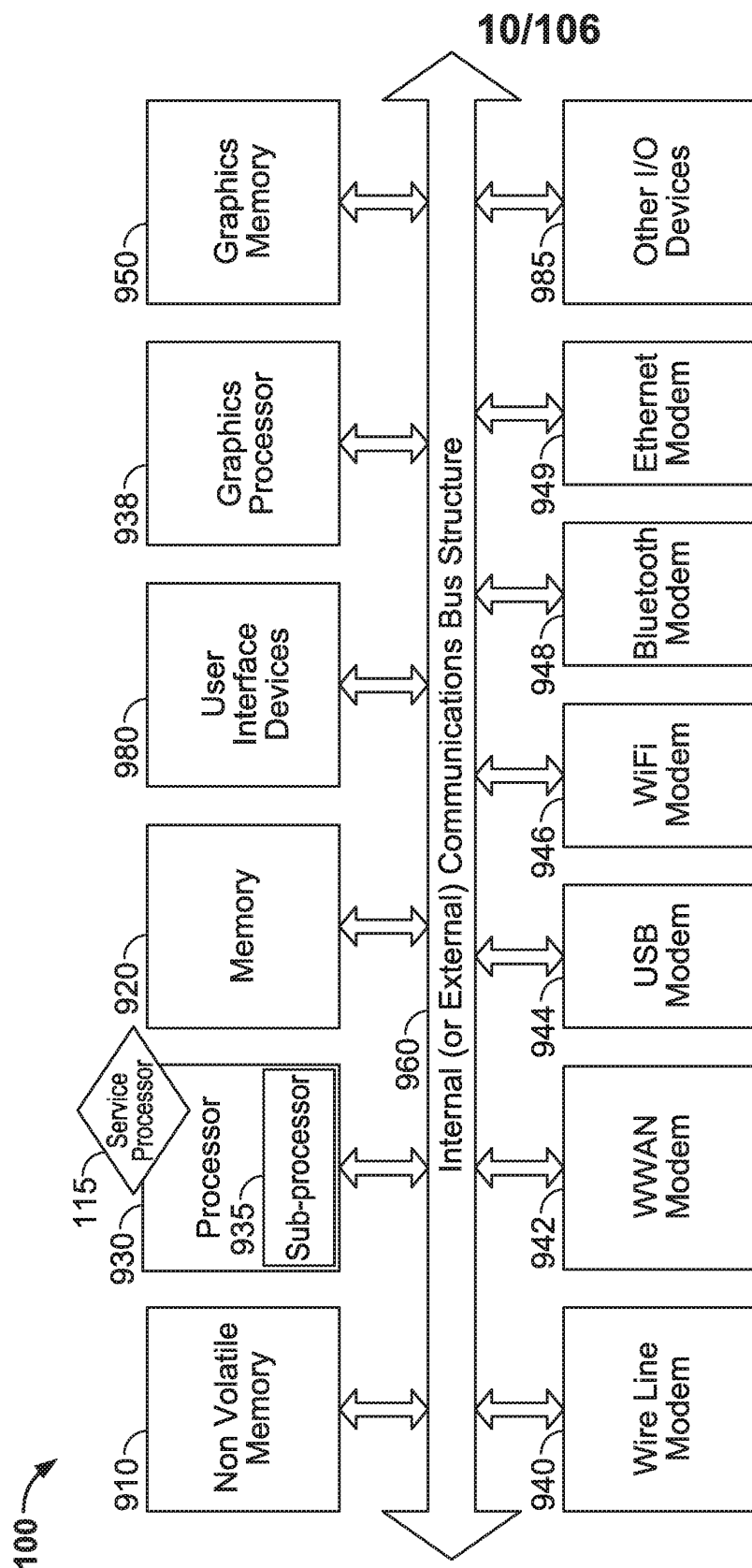


FIG. 10

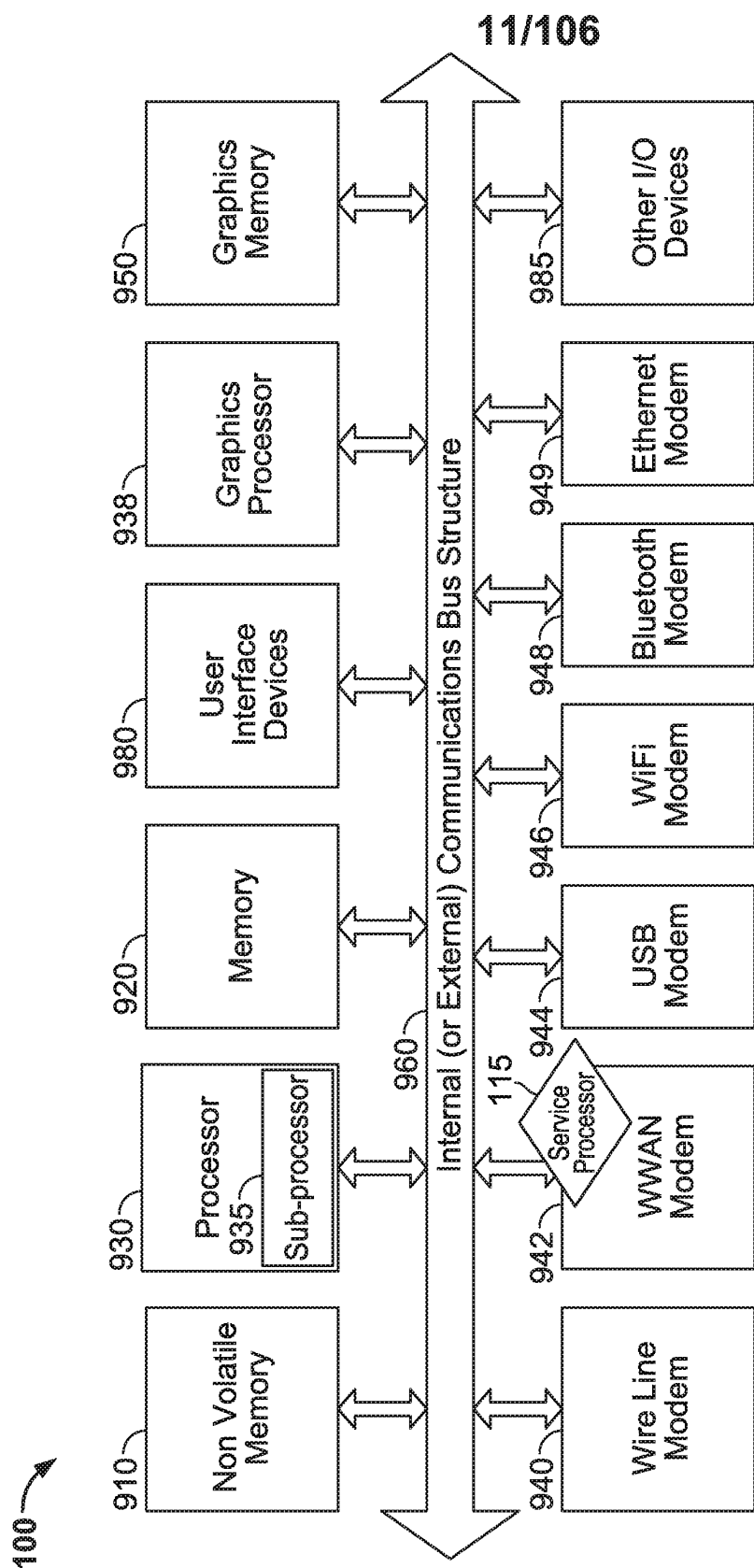


FIG. 11

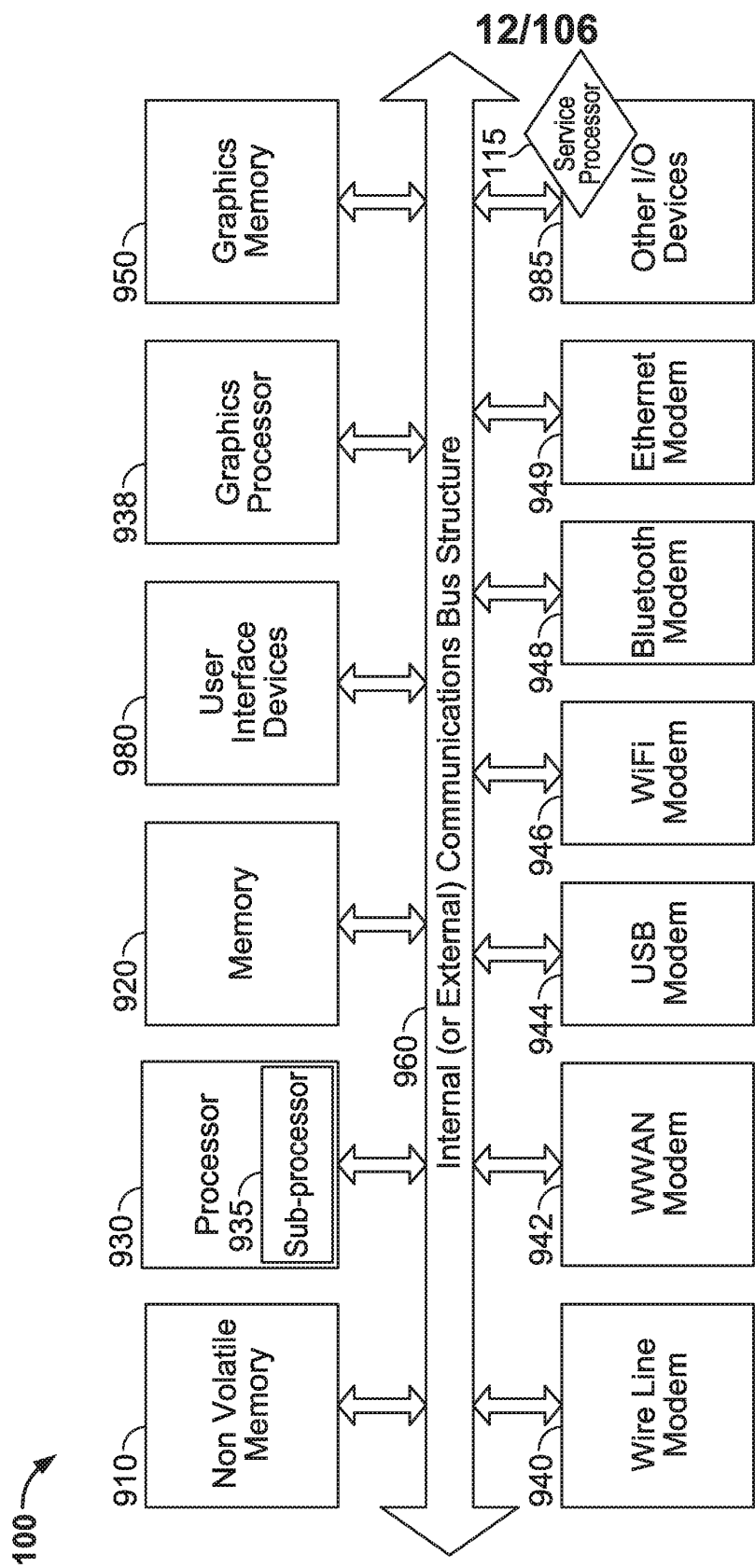


FIG. 12

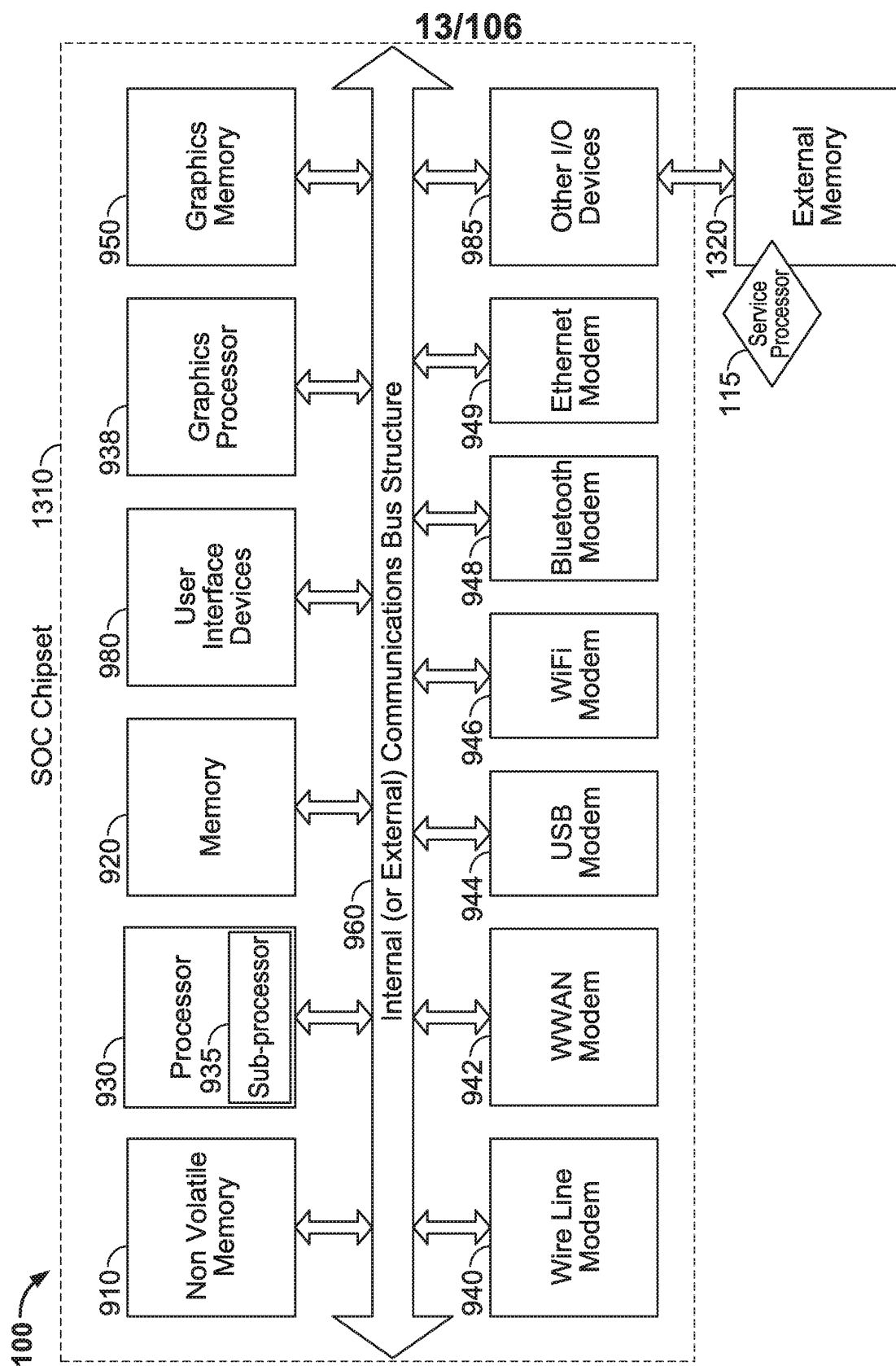


FIG. 13

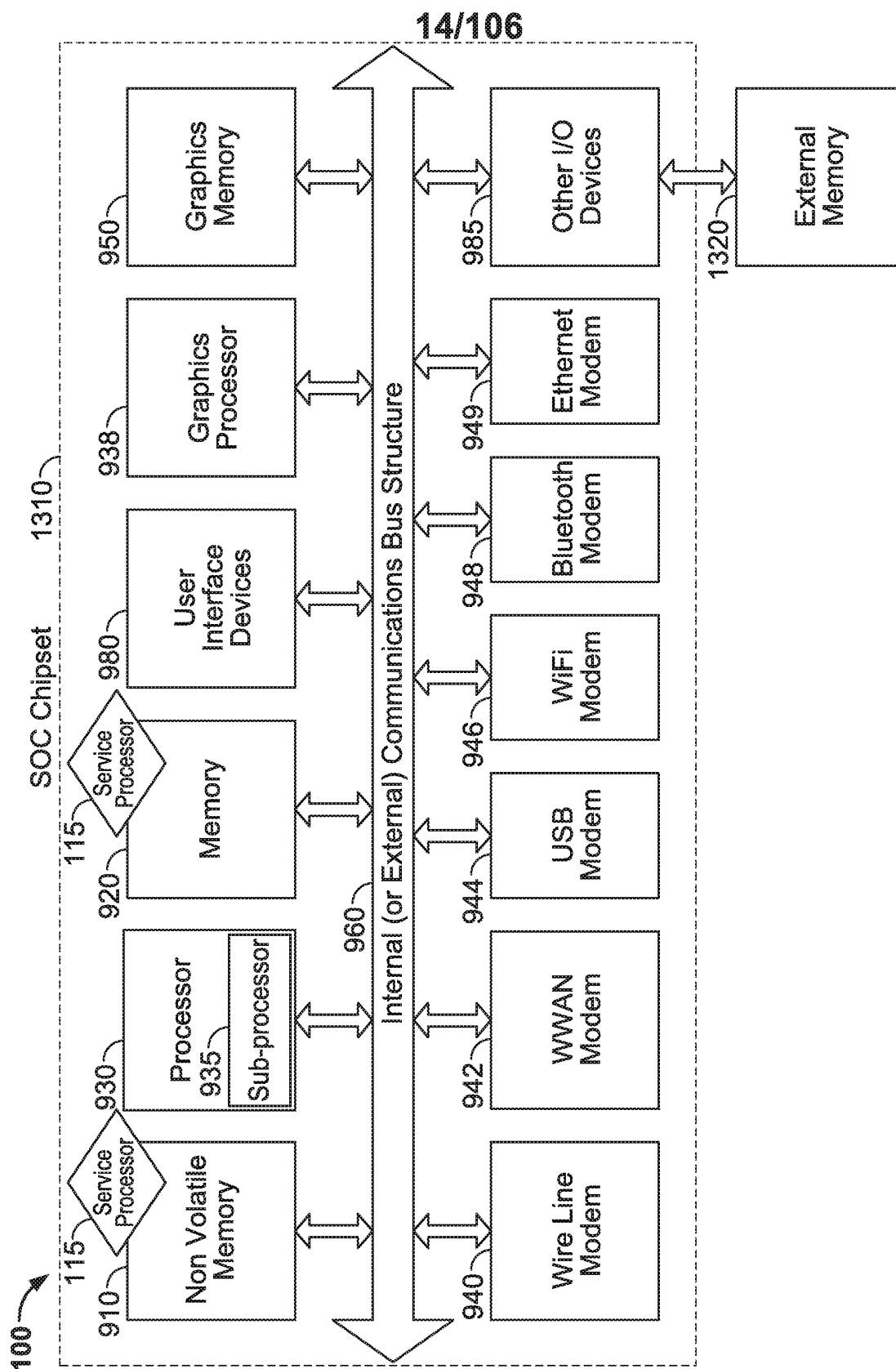


FIG. 14

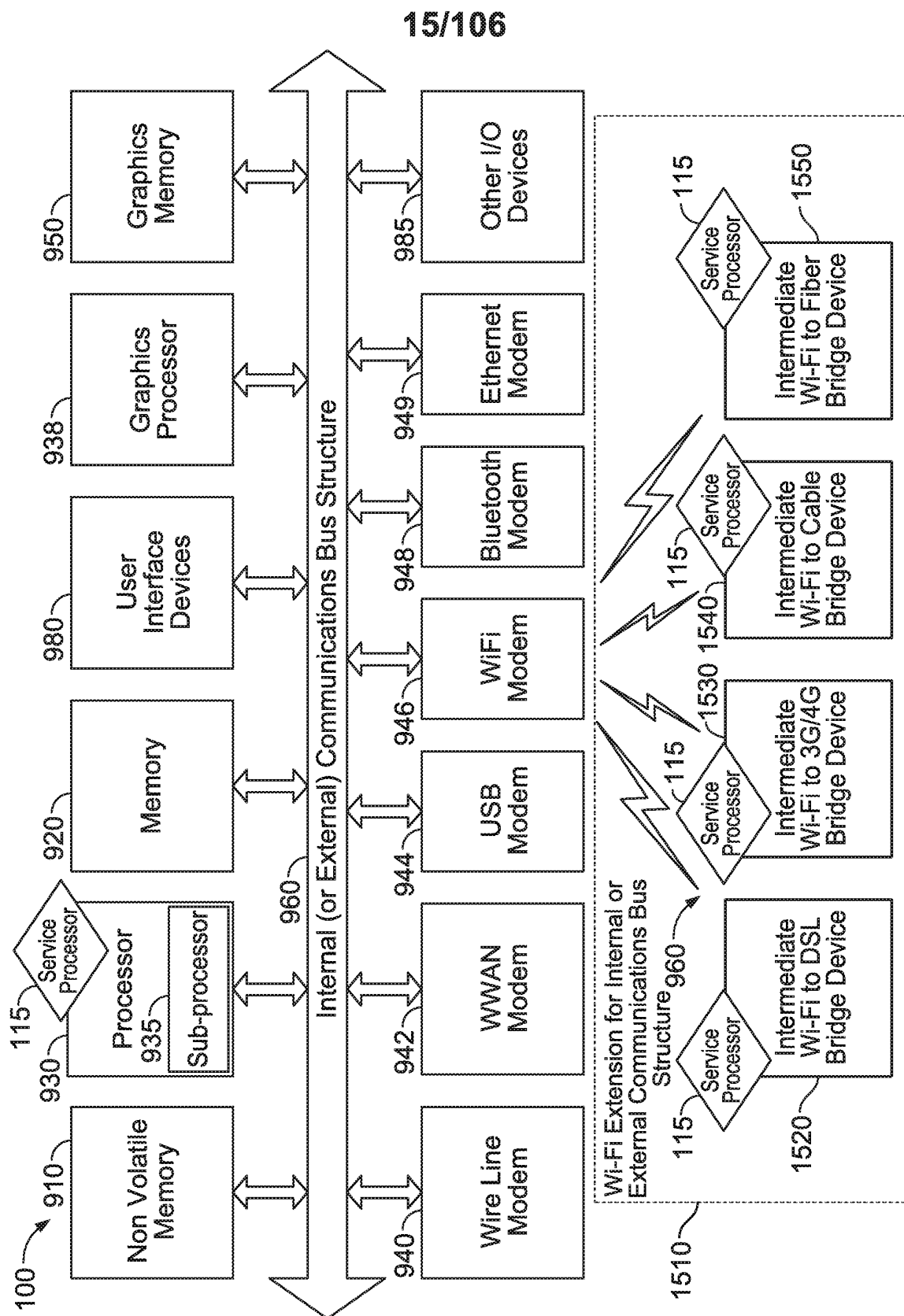


FIG. 15A

16/106

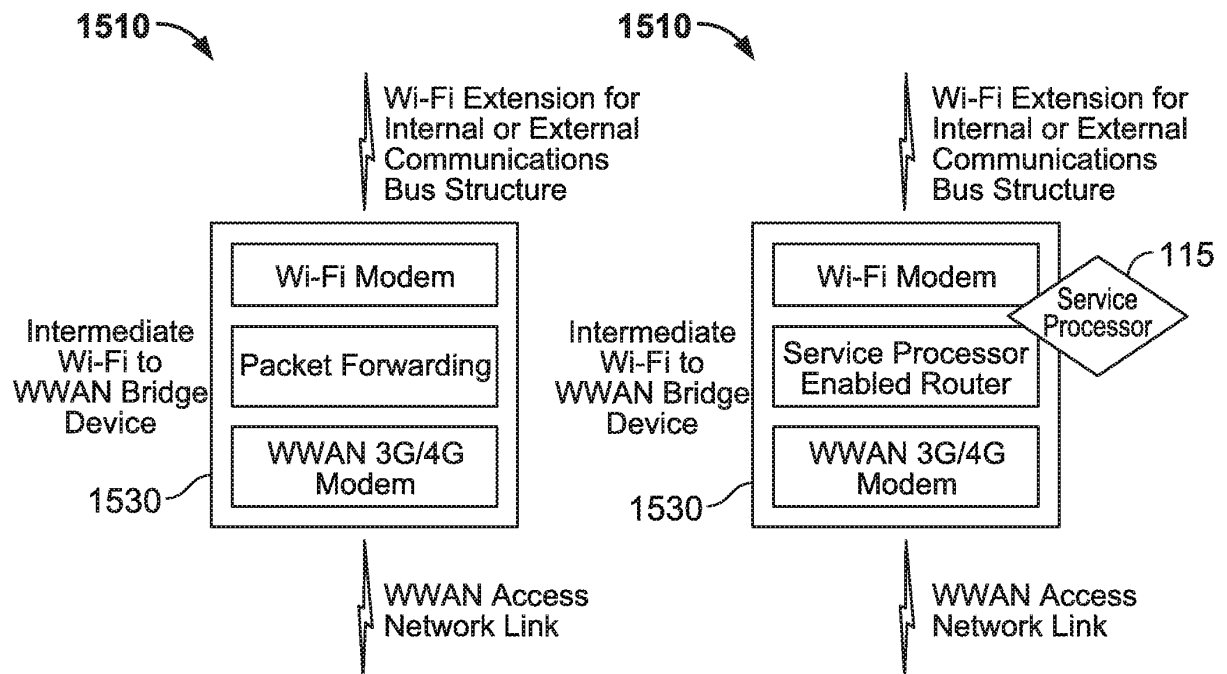


FIG. 15B

FIG. 15C

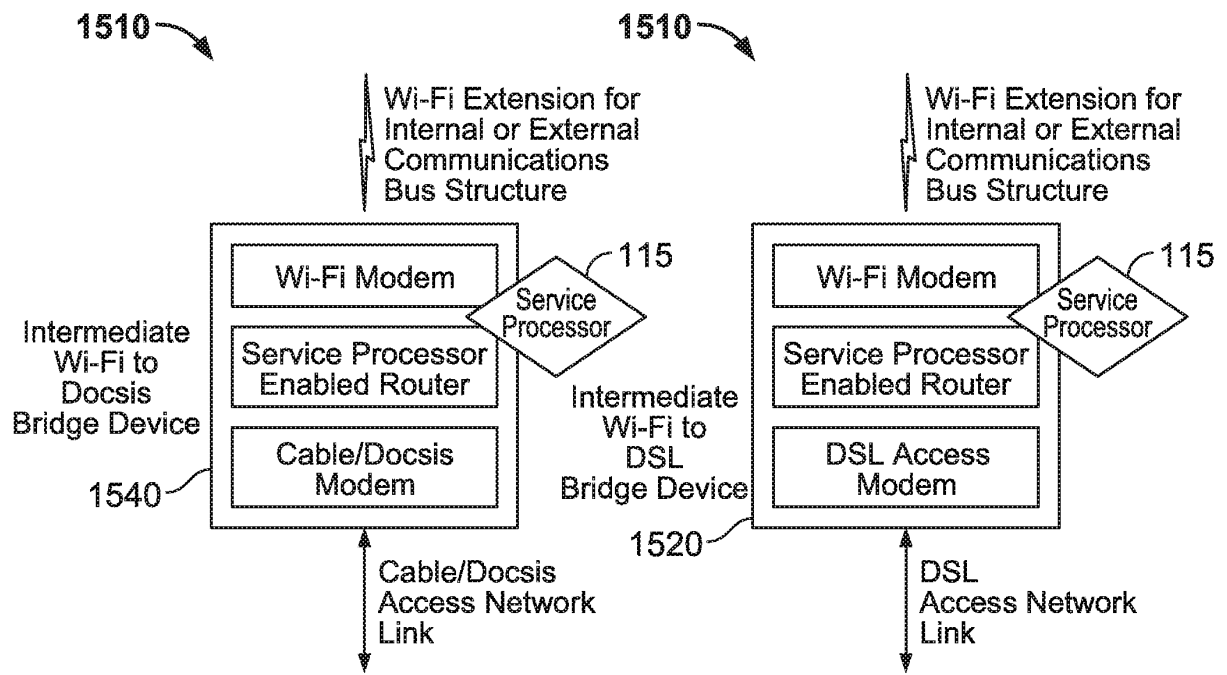


FIG. 15D

FIG. 15E

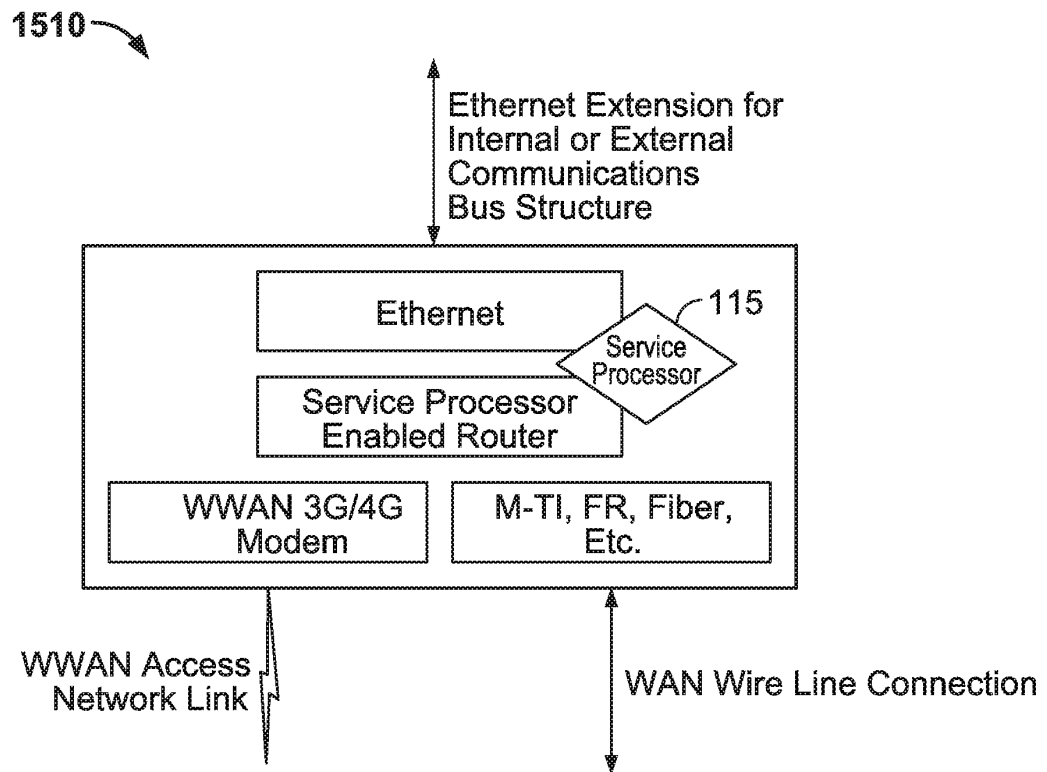


FIG. 15F

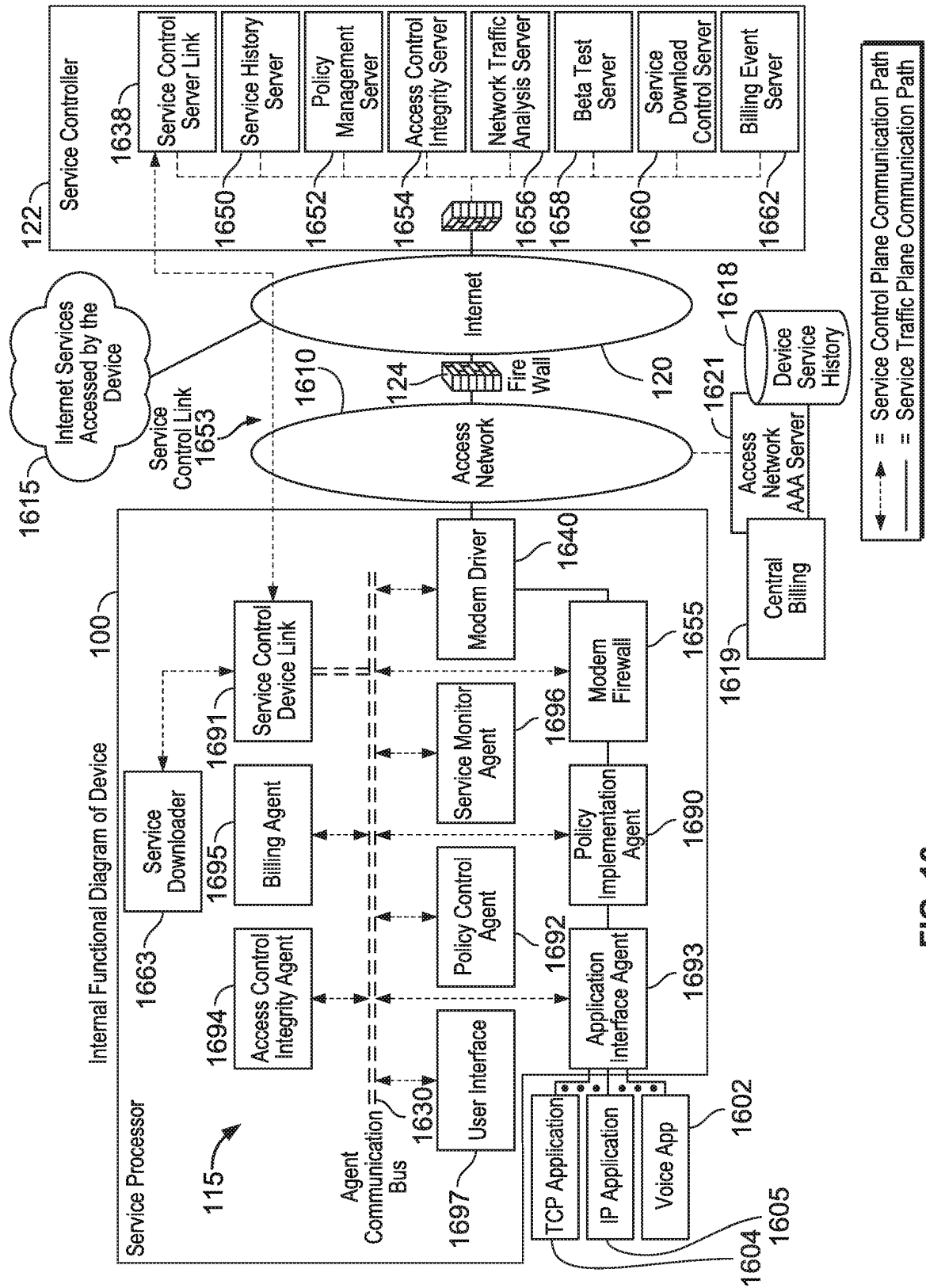
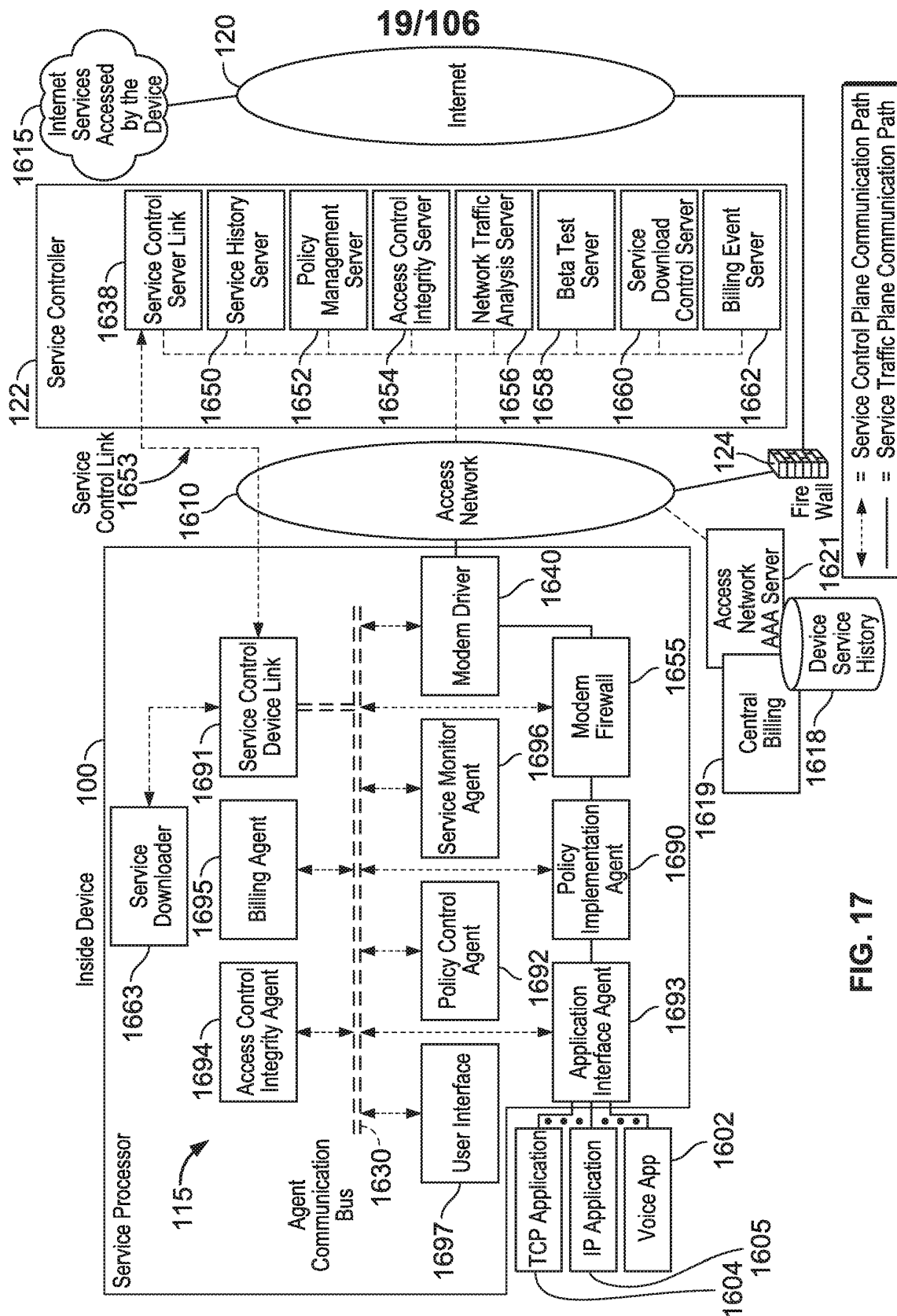
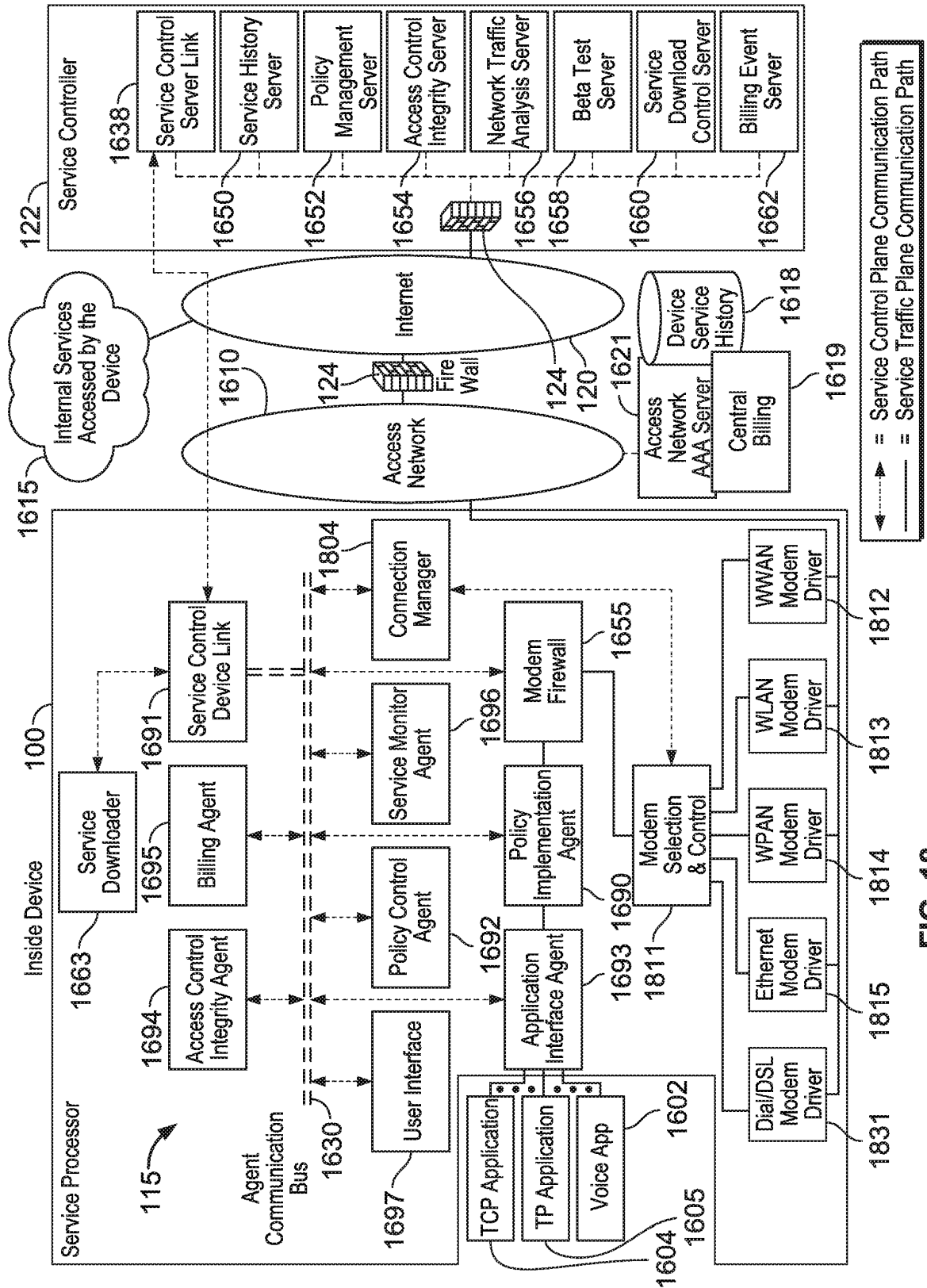


FIG. 16





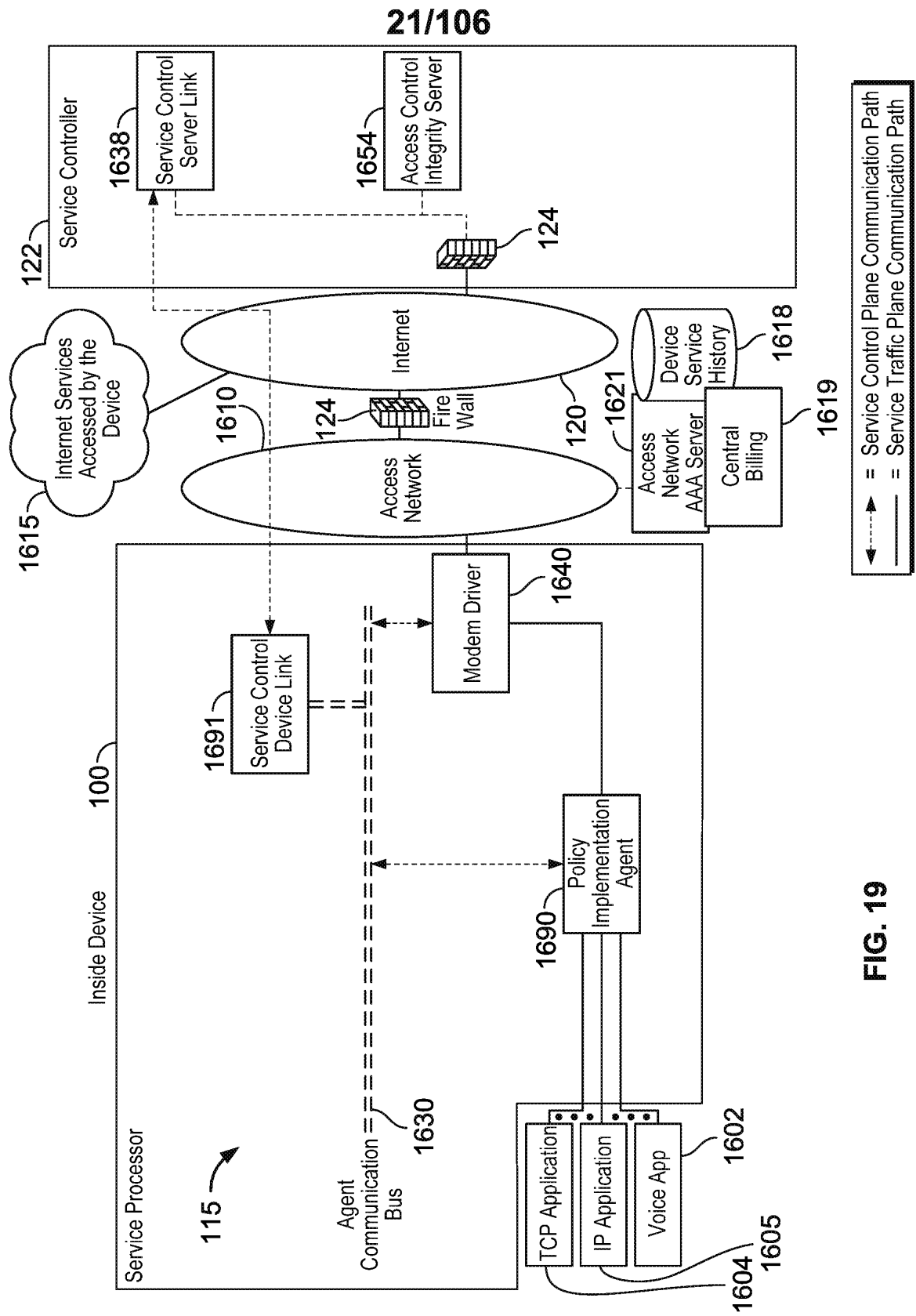
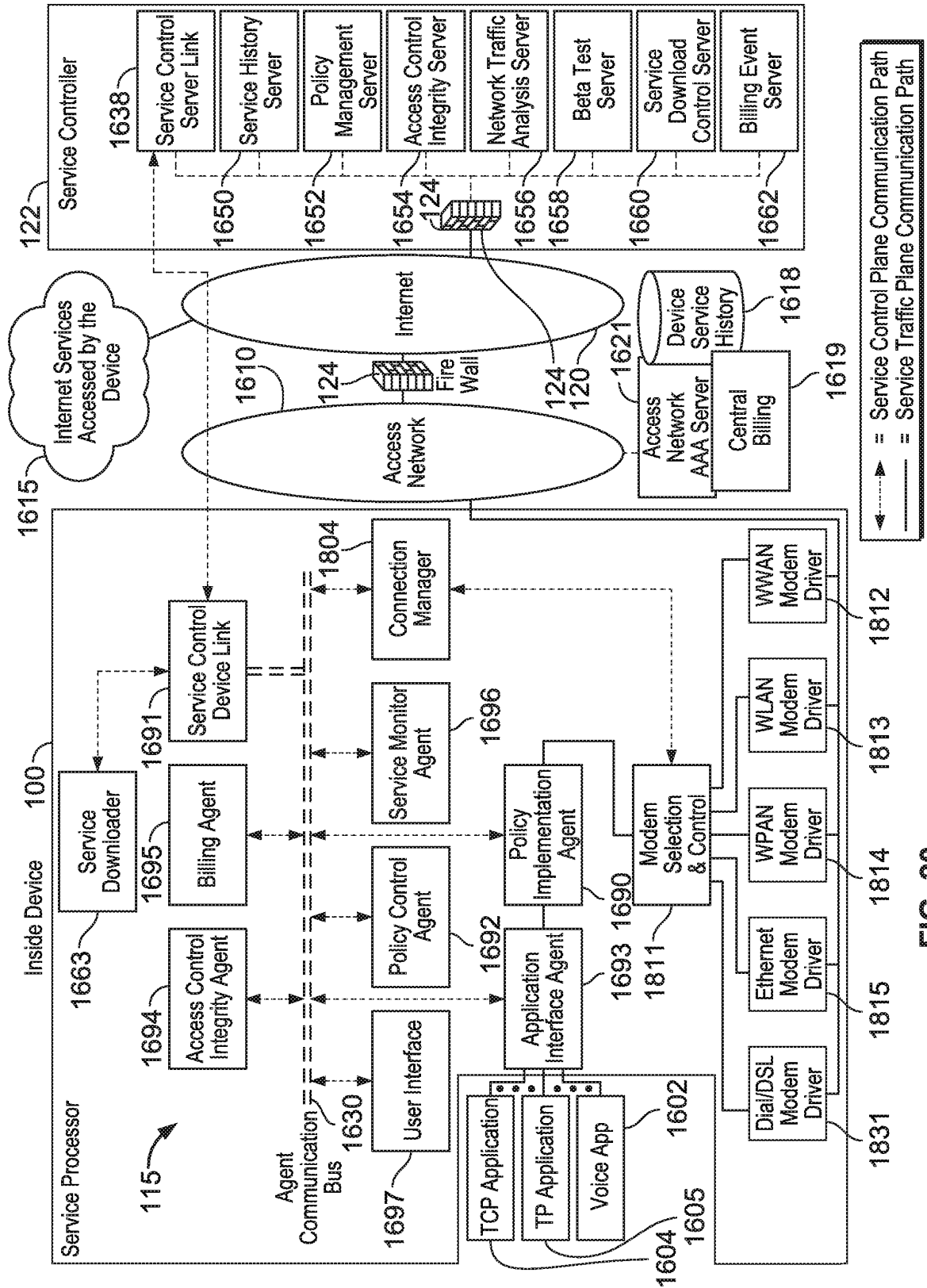


FIG. 19



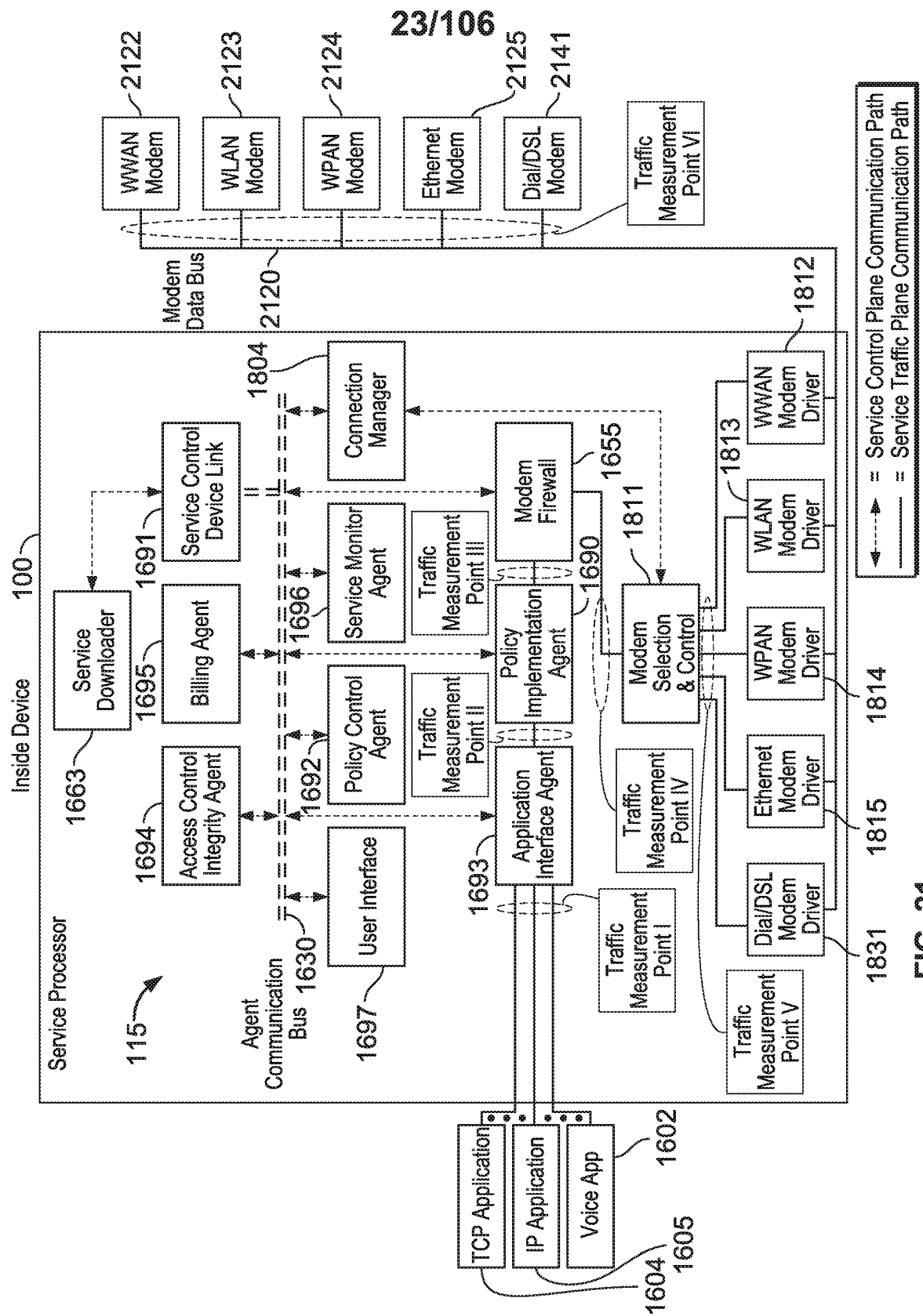


FIG. 21

Service Processor 115 Embodiment	Partial Summary of Embodiment Functions
Service Control Device Link 1691	Device side control plane link for connecting Service Processor 115 to Service Controller. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Agent 1694	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, verifies configuration of other agents or performs challenge-response testing. In some embodiments, monitors software loading activity, protected memory access or communication with Service Processor agents to detect unauthorized changes to Service Processor software or configuration.
Policy Control Agent 1692	Takes policy instructions from the network and sets instantaneous device service policy. In some embodiments, performs a policy control function to adapt instantaneous service policies to achieve a service usage objective.
Policy Implementation Agent 1690	Implements traffic control and QOS policy rules for device. In some embodiments provides the functions of access control and/or firewall function or perform traffic inspection and characterization. In some embodiments packet inspection is aided by literal or virtual application layer tagging while in other embodiments packet inspection is performed completely in the Policy Implementation Agent 1690.
Service Monitor Agent 1696	Records and reports device service usage. In some embodiments, assists in communicating application tagging of traffic flows through the networking stack policy implementation. In some embodiments, maintains a history and provides reports or summary reports of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection.
Application Interface Agent 1693	Rich feature interface for device application programs. In some embodiments, identifies application level traffic, reports service usage or tags traffic for service QOS control. In some embodiments, interacts with applications or programs applications to arrange application settings such as email file transfer options or browser headers. In some embodiments, intercepts certain application traffic to modify traffic application layer parameters such as email file transfer options or browser headers. In some embodiments implements certain aspects of traffic control or other service policies. In some embodiments, provides the functions of traffic control, access control and/or firewall.
Modem Firewall 1655	Blocks or passes traffic based on service policies and traffic attributes. In some embodiments, assists in traffic flow tagging. In some embodiments provides the functions of traffic control and/or access control.
Billing Agent 1695	Detects and reports billing events. In some embodiments interacts with the User Interface Agent 1697 to provide the user with service plan options, accept service plan selections, provide notification on service usage levels, provide options on service usage control policy, accept choices on service usage policy, provide transaction options or accept transaction choices. In some embodiments, interacts with Transaction Servers 134 to conduct ecommerce transactions with central billing.

FIG. 22A

User Interface Agent 1697	Provide service interface to users.
Service Downloader 1663	Provides a download function to install or update service software elements on the device.
Connection Manager 1804	Provides a control and supervision function for one or more modem drivers or modems that connect to an access network.
Modem Selection and Control 1811	Selects the access network connection.
Modem Drivers 1831, 1815, 1814, 1813, 1812	Converts data traffic into modem bus traffic for one or more modems.
Modems 2141, 2125, 2124, 2123, 2122	Connects the device to one or more networks.

FIG. 22B

Partial Summary of Embodiment Functions	
Service Controller 122 Element	
Service Control Server Link 1638	Network side control plane link for connecting Service Controller 122 Service Processor 115 device agents. In some embodiments, also serves as the link for the agent heartbeat function.
Access Control Integrity Server 1654	Collects device information on service policy, service usage, agent configuration and agent behavior. Cross checks this information to identify integrity breaches in the service policy implementation and control system. Initiates action when a service policy violation or a system integrity breach is suspected.
Policy Management Server 1652	Transmits policies to the Service Processor 115.
Access Network AAA Server 1621	Provides access control and authorization functions for the device access layer. Records and reports device network service usage.
Service History Server 1650	Collects and records service usage reports from the Access Network AAA Server 121 and the Service Monitor Agent 1696. In some embodiments, maintains a history of which networks in addition to the networks controlled by the Service Controller that the device has connected to. In some embodiments, this network activity summary may include a summary of the networks accessed, activity vs. time per connection, traffic vs. time per connection. In some embodiments, this activity summary is further analyzed or reported to estimate the type of service plan associated with the traffic activity for the purpose of bill sharing reconciliation.
Central Provider Billing System 1619	Provides mediation function for central provider billing events. Accepts service plan changes. In some embodiments, provides updates on device service usage, service plan limits or service policies.
Billing Event Server 1662	In some embodiments, collects billing events, provides service plan information to the Service Processor 115, provides service usage updates to the Service Processor 115, serves as interface between device and central Provider Billing System 123, or provides trusted third party function for certain ecommerce billing transactions.
Network Traffic Analysis Server 1656	Collects service usage history for devices or groups of devices and analyses the service usage. In some embodiments, presents service usage statistics in various formats to identify improvements in network service quality or service profitability. In other embodiments, estimates the service quality or service usage for the network under variable settings on potential service policy. In other embodiments, identifies actual or potential service behaviors by one or more devices that are causing problems for overall network service quality or service cost.
Beta Test Server 1658	Publishes candidate service plan policy setting to one or more devices. In some embodiments, provides summary reports of network service usage or user feedback information for one or more candidate service plan policy setting. In some embodiments, provides a means to compare the beta test results for different candidate service plan policy settings or select the optimum candidates for further setting optimization.
Service Download Control Server 1660	Provides a download function to install or update service software elements on the device.
Transaction Server 134	Provides an electronic commerce offering and transaction platform to the device.

FIG. 23

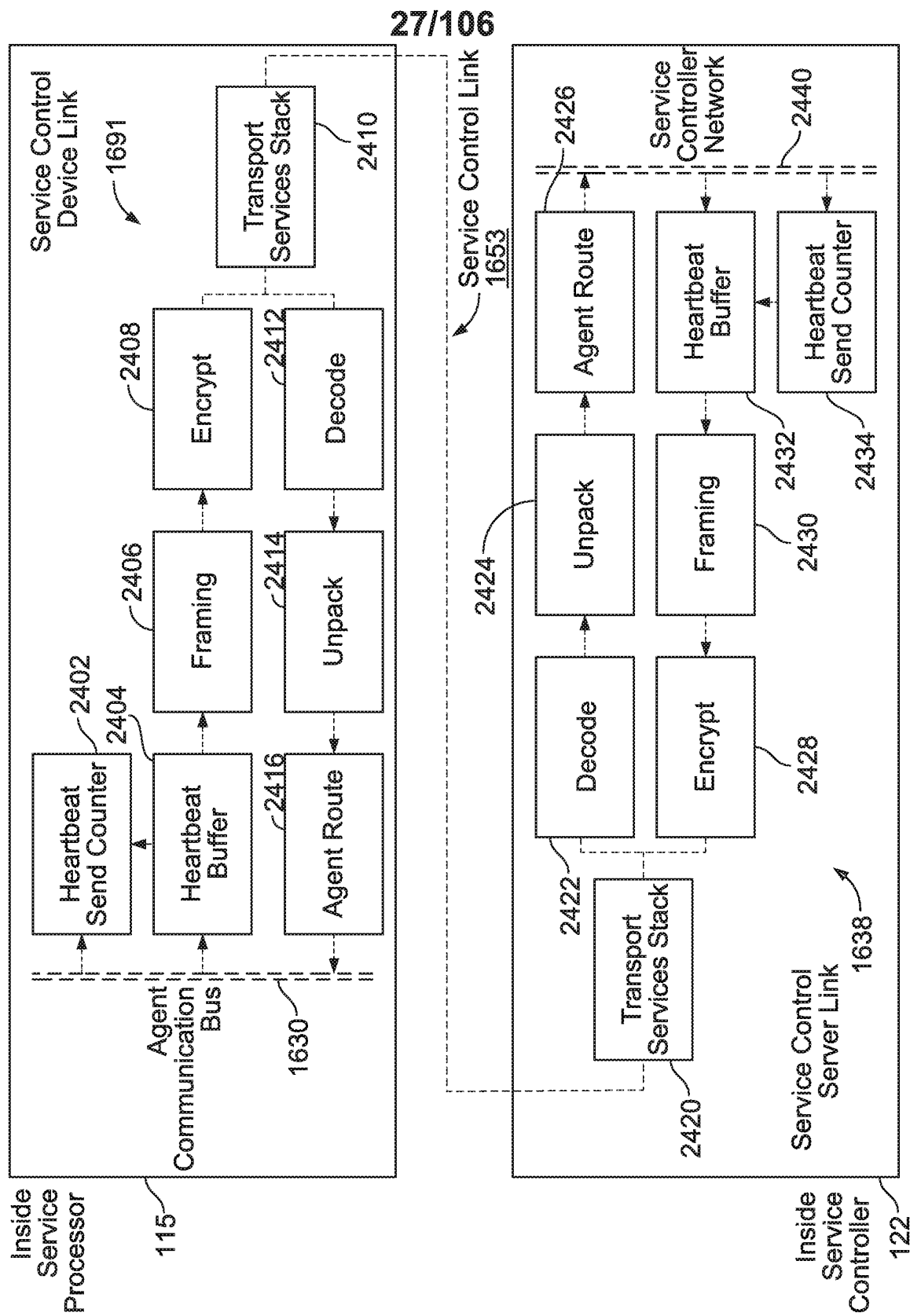
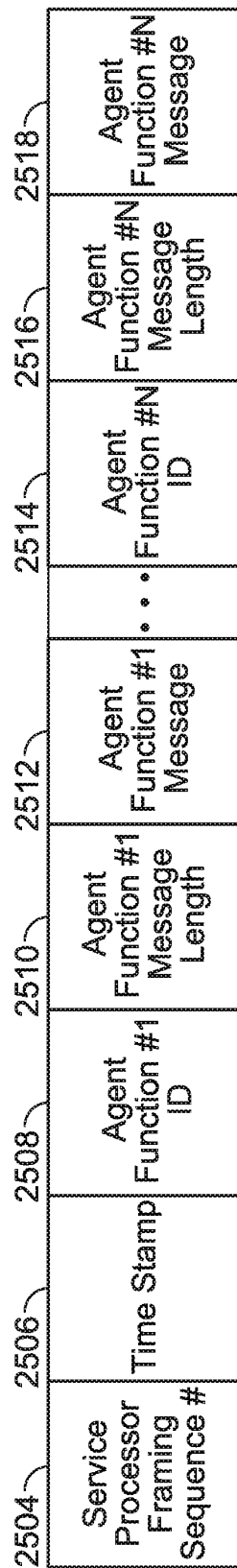
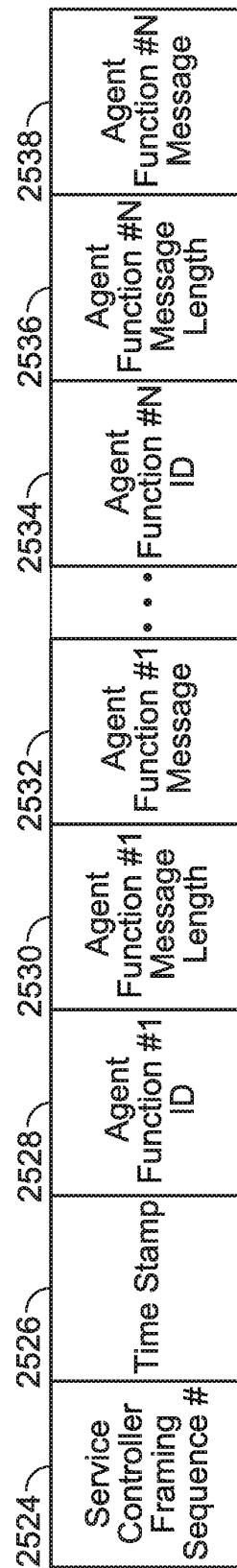


FIG. 24



Service Processor Communication Frame 2502

28/106



Service Controller Communication Frame 2522

FIG. 25

Example Service Processor Heartbeat Parameter Embodiments	Description	Frequency
Access control integrity report	Contains the latest results of the Access Control Integrity agents Service Processor system checks and reports any error events.	Not necessary to report in every heartbeat if there are no errors. Can report only on error, set a minimum frequency or respond to Service Controller polling.
Service monitor report	Reports filtered summary of Service Monitor Agent measurements. Summary reduces control traffic and filters out unauthorized private information.	Every heartbeat. Some embodiments link this to amount of data usage in the data path to keep overhead low. Report immediately upon polling from Service Controller.
Billing event report	Reports any billing activity since the last heartbeat. Billing events may include service usage events, transaction events, bill by account records, bill by account offset reports or any other event that results in a billing event report.	Send upon billing event. Report immediately upon polling from Service Controller.
Service Processor settings report	Reports service policy settings for all Service Processor agents.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Customer resource management report	Reports filtered summary of Service Monitor Agent measurements or filtered summary of other device or user activity such as service preferences, advertisement behavior and location. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments link this to amount of data usage to reduce overhead. Can report every N heartbeats. Report immediately upon polling from Service Controller.
Responses to Service Processor agent queries	Sends agent responses to challenge-response queries from the Service Controller.	Report immediately upon polling from Service Controller.

FIG. 26A

Location tracking service update	Reports filtered summary of location tracking information. Summary reduces control traffic and filters out unauthorized private information.	Not necessary to send every heartbeat. Some embodiments call for a minimum time based transmission frequency.
Service usage based transmission frequency	Lowers overhead by buffering and reserving heartbeat communications from agents and servers until a certain amount of data has been transmitted or received in the network, or a certain amount of service has been consumed. When the parameters are chosen properly, this can result in the network control plane traffic overhead being a small percentage of data path traffic or result in the control plane traffic cost being a small percentage of the service usage cost.	Ranges depending on settings. For example, if there are 5 agents messages that typically need to be communicated, and each message is less than 100 bytes, and Service Processor heartbeat framing plus network overhead would result in a packet size of less than 1,000 bytes, and the heartbeat packet is transmitted when 10,000,000 bytes have been communicated over the data path, then the overhead loss due to one heartbeat packet in each direction is less than 0.02%.
Constant frequency transmissions	Since the device may be off line for long periods of time where the Service Control Processor needs to verify service control integrity, in some embodiments it can be advantageous to transmit heartbeat packets at a minimum rate regardless of data traffic activity. This is accomplished by setting a timer that sends queued heartbeat packets on a regular schedule.	Ranges depending on settings and applications.
Service Controller polled transmissions	In some embodiments, the Service Controller may poll the Service Processor for a heartbeat transmission at which time the Service Processor will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Controller.
Service Processor polled transmissions	In some embodiments, the Service Processor polls the Service Controller for a heartbeat transmission at which time the Service Controller will frame and transmit all queued heartbeat messages.	Ranges depending on applications. In some embodiments this is used as an on demand function while in others it is used as a way to set heartbeat transmission timing functions in the Service Processor.

FIG. 26B

Agent self-check reports	Agent reports results of various agent self-diagnosis procedures to ensure that the agent is properly configured, operating properly, properly implementing service control policy or has not been tampered with. [provide examples which are extensions of typical software security self diagnosis reporting]	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Environment reports	One or more agents scan the storage or execution environment for one or more of the agents to identify potential threats to the integrity of the service implementation or agent integrity and makes a report. In one example embodiment, a scan is done to determine if unauthorized software or hardware is executing in a secure agent environment. In another embodiment, a scan is done to determine the software that has been loaded into a portion of the device operating environment, memory or storage, and the software list is referenced against a known threat list. In another example embodiment, the list of entities that accessed one or more agents is scanned to determine if an unauthorized access to an agent has occurred. In another embodiment a scan is performed to determine if unauthorized access to secure execution environment, memory or storage has occurred. In another example embodiment, the network access pattern for the device is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity. In another example embodiment, the internal device software, memory or peripheral access pattern is logged and analyzed to determine if there is an access pattern that is known to be associated with a threat to service or agent control integrity.	In some embodiments an report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.

FIG. 26C

User notification response reports	Billing agent, UI agent or another agent logs user notification events and the response of the user to the notification event. In some embodiments these events may be cross-referenced to the notification policy that should be in force on the device and the device service usage to ensure that the proper notification sequences are being adhered to. In other embodiments, the user notification responses are logged and used to document user choices to notification events, billing event decisions, service control decisions or service cost control decisions. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly. In some embodiments, the user may be asked to acknowledge a service overage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service overage acknowledgement.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a user notification sequence action with the user. In some embodiments, the report is generated when there is a verification error of some kind that is identified.
User warning response reports	Billing agent, UI agent or another agent logs user warning events and the response of the user to warning event. In some embodiments the user response is used to determine if the user is in positive control of the device. In some embodiments the response is used to confirm that the user acknowledges a billing overage or other service cost event. In some embodiments, the user may be asked to provide a password, biometric signature, hardware key or other mechanism to positively identify that the user is in possession of the device or to verify that the service is operating properly or is implemented properly.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device, for example when there has been a warning sequence action with the user. In some embodiments the report is generated when there is a verification error of some kind that is identified.

FIG. 26D

Agent communication log reports	Reports entities that established or attempted to establish communication with the agents. In one embodiment, reports a list of entities and the number of times the entity communicated or attempted to communicate with the agent. In another embodiment, reports an error flag when unauthorized entities attempt to establish communication with an agent.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Service usage synchronization data	IPDR or other data that is used to synchronize the device service usage counters. In some embodiments the data is time stamped so that the service usage at a point in time may be reconciled between the local device usage count and the network based usage count, and then the local device usage count since the point in time may be used to estimate the present real-time usage count. In some embodiments, the service usage data from the device is used by the network as the actual service usage or billing data base for the device. In other embodiments, a bill by account function is included in the service usage synchronization data so that the service usage may be billed to different accounts other than a single or main user account.	Service usage synchronization is continuous with each heartbeat in some embodiments. In other embodiments service usage synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.
Service cost synchronization data	Information to reconcile a service cost estimate on the local device with a service cost count from a network based function. Similar to the service usage count, in some embodiments the service cost information is time stamped so that service cost at a point in time may be reconciled between the device and the network based function, and then a local measure of service cost may be used to estimate the present real-time service cost. In some embodiments the local service cost is determined by taking recorded billing events and looking up the cumulative cost of one or more billing	Service cost synchronization is continuous with each heartbeat in some embodiments. In other embodiments service cost synchronization is based on a push from the Service Controller or other network function that sends the IPDR information to the device. In other embodiments, the device requests a synchronization data transmission.

FIG. 26E

	events using a service usage to cost look up data base stored locally on the device or available from a network function. In some embodiments, service cost estimation is done entirely in the network and the result is pushed out to the device UI. In other embodiments service cost estimation is done in the device based on local usage estimates and a local usage to cost lookup table.	
Available network information and roaming information	<p>Device receives available network or available roaming service provider information from a network function. The available network or roaming service information may include the potential network service or roaming service a device or user may choose to select, or the network service or roaming service the user has already selected. In some embodiments this information includes service cost information to aid the device or the user in determining the potential or actual costs of service usage while using the available network or roaming network. In some embodiments the service cost information is used to help the user in selecting the available network provider or roaming service provider. In some embodiments the available network cost information or roaming cost information is combined with a measure of expected or possible service usage to estimate how much a typical usage scenario may cost. In some embodiments, the available network information or roaming information is used to help the user estimate the present available network or roaming service charges for services used to date. In some embodiments service usage is recorded and sent to a network function that estimates the current service cost. In other embodiments the service cost is estimated locally on the device based on a service usage estimate and a service usage to cost look up function. In other</p>	<p>In some embodiments available network information or roaming information is requested by the device. In other embodiments, the information is periodically updated by the Service Controller or other network function that contains the information.</p>

FIG. 26F

	embodiments, the service cost is derived by querying the available network or roaming network billing system.	
System messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display a system messages or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include, etc.	System messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments, some system messages are generated in response to user input or requests. In other embodiments, system messages are generated on a regular time table or in accordance with a certain amount of service usage.
UI screen messages and responses	In some embodiments the heartbeat function may be used as a secure control channel to display user interface message or screen that is generated by a network function or server to the end user and possibly report user inputs to the UI message or screen. Examples include service usage UI, service choice UI, upgrade UI, transaction UI, marketing UI, billing UI, user identify confirmation UI, user service warning UI, user potential service tamper response request UI, etc.	UI screen messages are generated by the Service Controller and transmitted as needed in some embodiments. In other embodiments some user UI messages are generated in response to user input or requests. In other embodiments, UI messages are generated on a regular time table or in accordance with a certain amount of service usage.
Local agent check-in history	Logs and reports agent check-ins or self-reports that are made to a local agent integrity verification function.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified.
Software install report	Logs and reports one or more aspects of software installs that have occurred on the device.	In some embodiments a report is made during every heartbeat transmission. In other embodiments the report is generated by a request from the Service Controller. In other embodiments the report is generated by timing determined by the device. In some embodiments the report is generated when there is a verification error of some kind that is identified. In some

FIG. 26G

		embodiments, the report is generated when new SW is installed.
Test billing event	In some embodiments the Service Controller or other network function may send or cause a test billing event wherein the device triggers a local billing sequence for the purpose of verifying that the billing sequence is properly logged, conducted and reported. The billing sequence can be related to a service usage event or sequence, a transaction event or sequence, or any other event or sequence that should result in a billing event.	In some embodiments, the test billing event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.
Test service event	In some embodiments the service Controller or other network function may send or cause a service usage event wherein the device triggers a local service usage event or sequence for the purpose of verifying that the service usage event or sequence is properly logged and reported.	In some embodiments, the test service usage event timing is determined by the Service Controller or other network function. In others it is generated by the device or on a regular schedule.

FIG. 26H

Service Policy Implementation Verification Technique Embodiments	Example Error Trigger Criteria Embodiments	Example Error Response Embodiments
<p>Verify service usage measure in network is consistent with expected service behavior</p>	<p>Network service usage measure is in conflict with expected service usage. Examples: traffic usage outside limits, address access outside limits, data rate outside limits, traffic shaping rules not being followed.</p>	<p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of the other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if errors persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service inspection process, or usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>

FIG. 27A

Verify service usage measure at device is consistent with expected service behavior	Device service usage measure is in conflict with expected service usage. Examples: traffic usage too high, address access outside limits, email accessed against policy.	Same as above.
Verify service usage measure in network is consistent with service usage measure at device	Device service usage measure varies significantly from network service usage measure	Same as above.
Verify service usage measure at one point in device is consistent with service usage measure at a second point in device	Service usage measure at one point in device stack that is inconsistent with another point indicates error or potential parasitic usage	Same as above. In some embodiments, the differences in service measures on the device may be used to evaluate the nature of the service usage policy implementation problem.
Verify that service policies in effect are as intended	Service policy setting queries result in settings that are different than intended	<p>In some embodiments, reset service policies and see if error persist. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition</p>

FIG. 27B

Verify presence of Service Processor agents	Agent does not respond to agent communication or query-response	<p>to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p> <p>In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify configuration of Service Processor agents	Agent configuration audit or configuration self check fails.	<p>In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the</p>

FIG. 27C

Verify billing events are reported or are reported properly		<p>error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source of error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify billing events are reported or are reported properly	Billing Agent query reveals logged billing events that have not been reported.	<p>In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service</p>

FIG. 27D

		<p>policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source of error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
<p>Verify network reported service usage measure are consistent with reported device billing data.</p>	<p>Billing agent is not properly reporting billing events for service usage, transactions, bill by account, or other billing event functions.</p>	<p>In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service</p>

FIG. 27E

		<p>policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify device reported service usage measure are consistent with reported device billing data.	Billing agent reports are inconsistent with service usage reports.	<p>In some embodiments, perform a billing event test to determine if the billing event reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, perform a service usage test to determine if the service usage reporting sequence is operating properly. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the</p>

FIG. 27F

		<p>appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
<p>Send test billing event through device and verify it is reported.</p>	<p>Test billing event is not properly reported by the device.</p>	<p>In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine</p>

FIG. 27G

		<p>agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a service usage test to determine if the device is properly reporting service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis</p>
<p>Verify device reports billing events reported from transaction servers.</p>	<p>Transaction server receipts do not correspond with billing events from device.</p>	<p>In some embodiments, perform checks to determine if transaction server receipts are valid. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if these are not the error correction methods employed, then perform one or more of the following actions:</p> <p>In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to</p>

FIG. 27H

		the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Verify activation tracking system presence, configuration or operation	Activation tracking service is not present, is not providing scheduled network activity reporting, or is exhibiting erroneous reports.	In some embodiments the response is to place the device ID, on a list of devices suspected of having activation tracking functions that have been tampered with for the purpose of central provider billing reconciliation. In some embodiments, install a new copy of the activation tracking service agent software either from a locally stored device copy or a network download. In some embodiments where authorization exists to manage device software and some aspects of service tracking, run further checks on device service integrity such as agent query-response. In some embodiments where authorization exists to manage a device access service connection, send error message to device UI, suspend device or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Verify device standing or service plan standing	No service plan on record or device not authorized	In some embodiments, if device is not yet activated with a service plan, provide UI with activation sequence. In some embodiments, if device is not authorized for service on one of the networks controlled by the Service

FIG. 271

Verify proper operation of Service Processor agents		Controller, send the UI an error message instructing the user how to proceed. In some embodiments, configure the Service Processor for the ambient service intended for that device. In some embodiments, download the appropriate Service Processor agent software that is appropriate for that device.
Check input to output relationship on Policy Implementation agent, Firewall agent. Check billing event reports to verify events are being recorded. Check application and traffic inspection tagging system correctly tagging traffic. Verify Service Processor heartbeat reports proper agent integrity self-checks, cross-checks and query/response sequences with Service Controller.		In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.

FIG. 27J

Service Processor heartbeat response reports	One or more of the heartbeat reports indicate an error in operation, configuration, or tamper and error prevention system. Heartbeat function not functioning properly but device is still indicating service usage on the network.	In some embodiments the severity of the error and/or the persistence of the error and/or the existence of other errors are used to determine the appropriate response or action. In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.
Test service event	Service usage reporting system does not properly report test service usage event	In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the

FIG. 27K

Load a fresh version of Service Processor software and perform integrity reports		<p>following actions:</p> <p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing test event to determine if the device is properly reporting billing events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Load a fresh version of Service Processor software and perform integrity reports	After fresh load of Access Control Integrity Agent, agent discovers one or more of the other agents are corrupted.	<p>Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a</p>

FIG. 27L

		<p>user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify Service Processor code configuration with agent self diagnosis checks	One or more of the agents indicates an error after running a self-check.	<p>Run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh other agents and see if problem persists. If this does not clear the error, or if this is not the error correction method employed, then perform one or more of the following actions:</p> <p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the</p>

FIG. 27M

Verify that device uses service only after being authorized		<p>device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify that device uses service only after being authorized	<p>Device gains access to the network and does not check in with the Access Control Integrity Server and service measures indicate device is on the network.</p>	<p>In some embodiments, reset service policies and see if error persists. In some embodiments, perform agent settings check to verify that agent service usage control policy settings are correct. In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control. In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, perform a billing event test or a service usage test to determine if the device is properly reporting billing events or service usage events. In some embodiments, the device is placed on</p>

FIG. 27N

		<p>quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
Verify user standing	User does not respond with proper response to UI query such as request for ID., password or biometric input. This process may be part of handling a suspected error.	<p>In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis. In some embodiments, the user may be asked to acknowledge a service coverage notification and/or to also provide a password, biometric signature, hardware key or other mechanism to verify the service coverage acknowledgment.</p>
Agent communications log	Unauthorized communications with one or more agents is detected	<p>In some embodiments, perform agent query/response to determine agent integrity. In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh one or more agents. In some embodiments, a user query or warning is sent to the UI to notify the user, confirm that the device is in the user's possession, or involve the user in the process of determining the source or error or to assist in verifying the device based service control.</p>

FIG. 270

		<p>In some embodiments, the device identification number is placed on an error list for further error handling. In some embodiments, the device is placed on a SPAN process, or a similar traffic or service inspection process, or another service usage watch status, to closely monitor service behavior and determine if it is consistent with the service usage policy that is intended to be in place. In some embodiments, the device is placed on quarantine network routing status, possibly with a user message being sent to inform the user. In some embodiments, the device service is suspended, possibly after sending the user a message that may include instructions on the process for correcting the error and resuming service. In some embodiments, the user messages are sent through an alternative messaging system, such as email or text messaging, as an alternative to or in addition to a message sent to the device. In some embodiments, an error message is sent to a human interface in the network for further error analysis.</p>
--	--	---

FIG. 27P

Service Policy Implementation Tamper or Error Protection Techniques	Example Error Trigger Criteria	Example Error Responses
Detect or block device networking activity that is potentially harmful for the operation of Service Processor.	Network activity is observed in service monitor reports that fit known patterns that indicated harmful software may be present on device.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized Service Processor software from being loaded.	Access Control Integrity Agent discovers software that is on a known malicious list.	Same as above.
Detect or block unauthorized access of protected Service Processor software or hardware memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detect or block unauthorized communication with Service Processor software or hardware.	Unauthorized communication is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

FIG. 28A

Secure loader with signed SW installed into protected memory	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor agents.	Secure communication link is in error or unauthorized access is detected.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments, run dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code to refresh agents with communication links that are in error or entire Service Processor. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Secure encrypted communication between Service Processor and Service Controller.	Service Processor communication is lost.	Send error message to device UI (if possible), suspend device, place on SPAN, place on watch list, place on further action list or place device on quarantine route. In some embodiments send error message to human interface for troubleshooting.
Execution of Service Processor software within secure memory.	Unauthorized access is detected, memory contents are corrupted or unresponsive.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.

FIG. 28B

Storage of service processor software in secure memory	Secure memory violation or Service Processor stored in non-secure memory	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Detection or removal of software thought to be harmful to Service Processor operation.	Unauthorized software is detected.	Initiate or install and initiate eradication software. Block traffic from the suspect entity. In some embodiments if software can not be eradicated or blocked, then send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Recording and reporting of software loading signatures, software activity signatures or network activity signatures for later identification of threat sequences.	Unauthorized software or malicious network activity is detected	Same as above.
Implement critical Service Processor software as a self-refreshing program that resists corruption by running self-audit and reinstall processes such as placing audit function in inaccessible memory or OS functions or bios.	Re-installation function alerts that Re-installation has been required. Continued re-installations or failure to re-install alert increases severity of warnings.	Identify the entity that has gained access to the Service Processor if possible and eradicate. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting.
Encrypted agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code encryption	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code . In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send

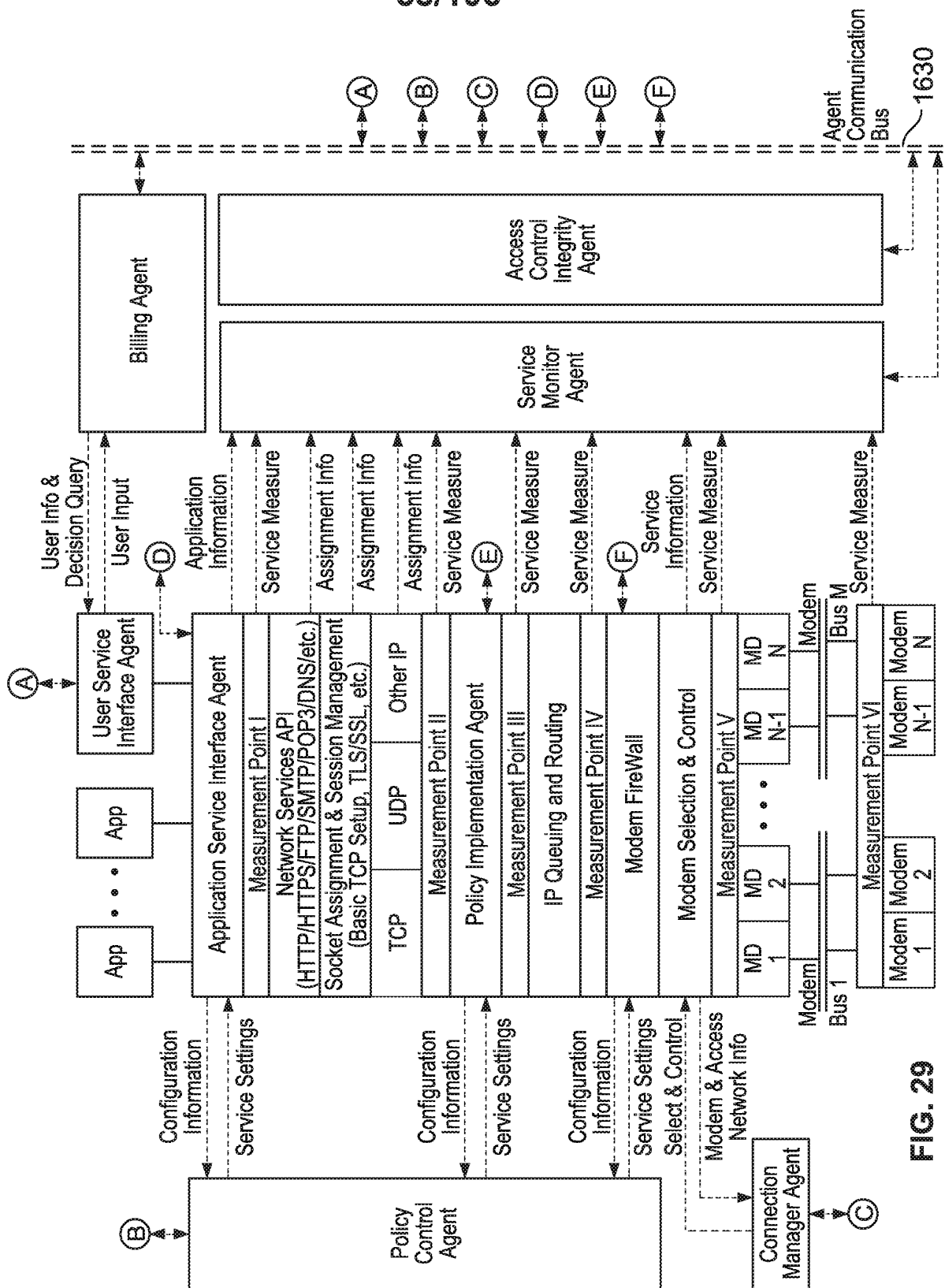
FIG. 28C

		error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Obfuscated agent code	Code check, agent query-response, agent self check or other agent configuration check discovers error in code obfuscation	Same as above.
Unique agent identification numbers and signatures	Agent is discovered to have an incorrect ID, or fails signature	Same as above.
Secure agent communication bus	Agent communication bus monitoring discovers unauthorized communication or other unauthorized access to one or more agents is discovered	Same as above.
Agent level message encryption	Agent is found to be communicating without the required level of agent communication encryption	Same as above.
Service control link message level encryption	Unauthorized communication traffic is discovered on service control link	In some embodiments repair any compromised agents with dynamic agent load, in some cases with different encryption, sequencing or obfuscation for the new agent code. In some embodiments send message to UI and either suspend device, place on SPAN, place on watch list, place on further action list or place on quarantine network. In some embodiments send error message to human interface for troubleshooting. Identify the entity that may have gained access to the Service Processor if possible and eradicate.
Service control link transport layer encryption	Unauthorized communication traffic is discovered on service control link	Same as above.
Agent communication access permissions	Unauthorized communication is discovered with one or more agents	Same as above.

FIG. 28D

Agent communication log	Unauthorized communication is discovered with one or more agents	Same as above.
Encrypted agent code for downloads	Agent download is found to have incorrect or absent encryption or signature	Same as above.
Secure downloader memory	Unauthorized access to or storage in secure downloader memory is discovered	Same as above.

FIG. 28E



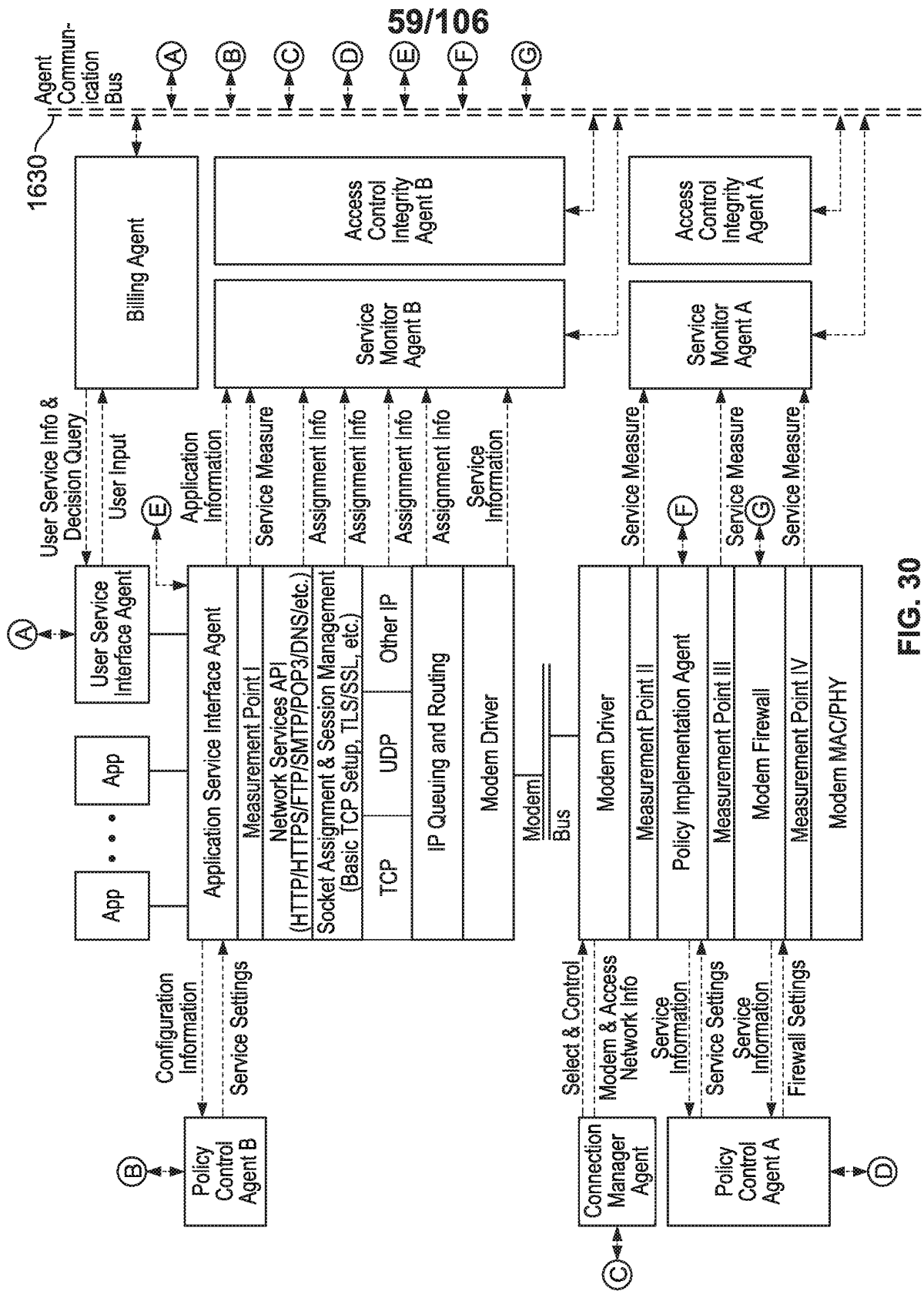


FIG. 30

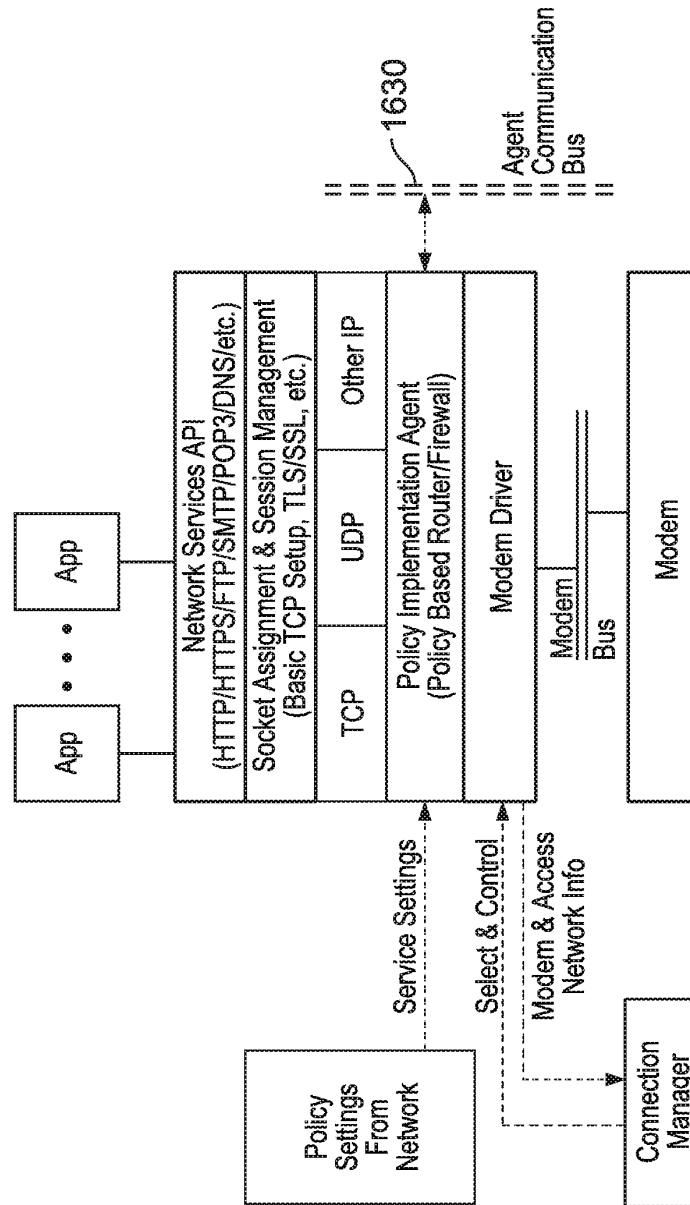


FIG. 31

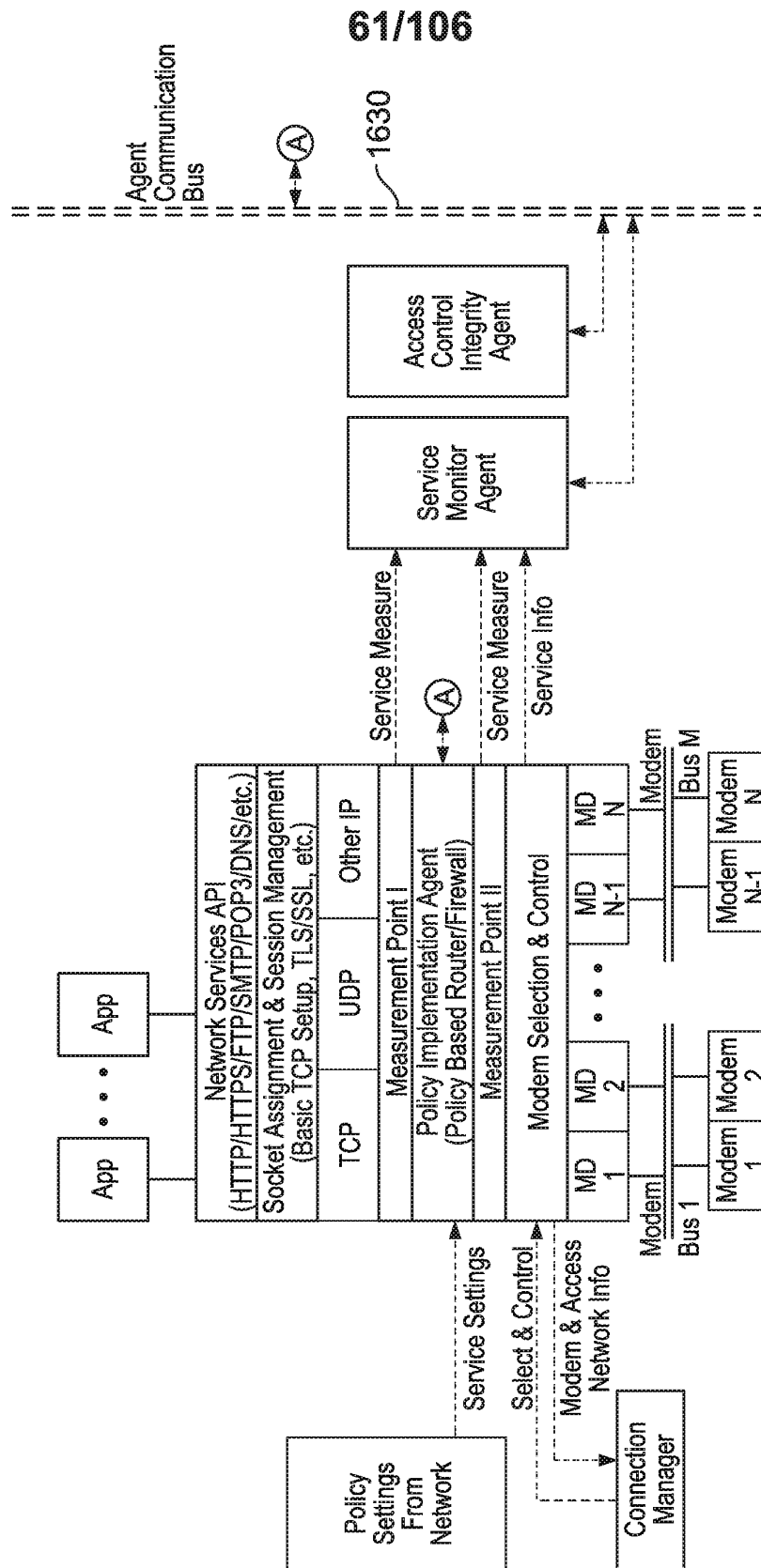


FIG. 32

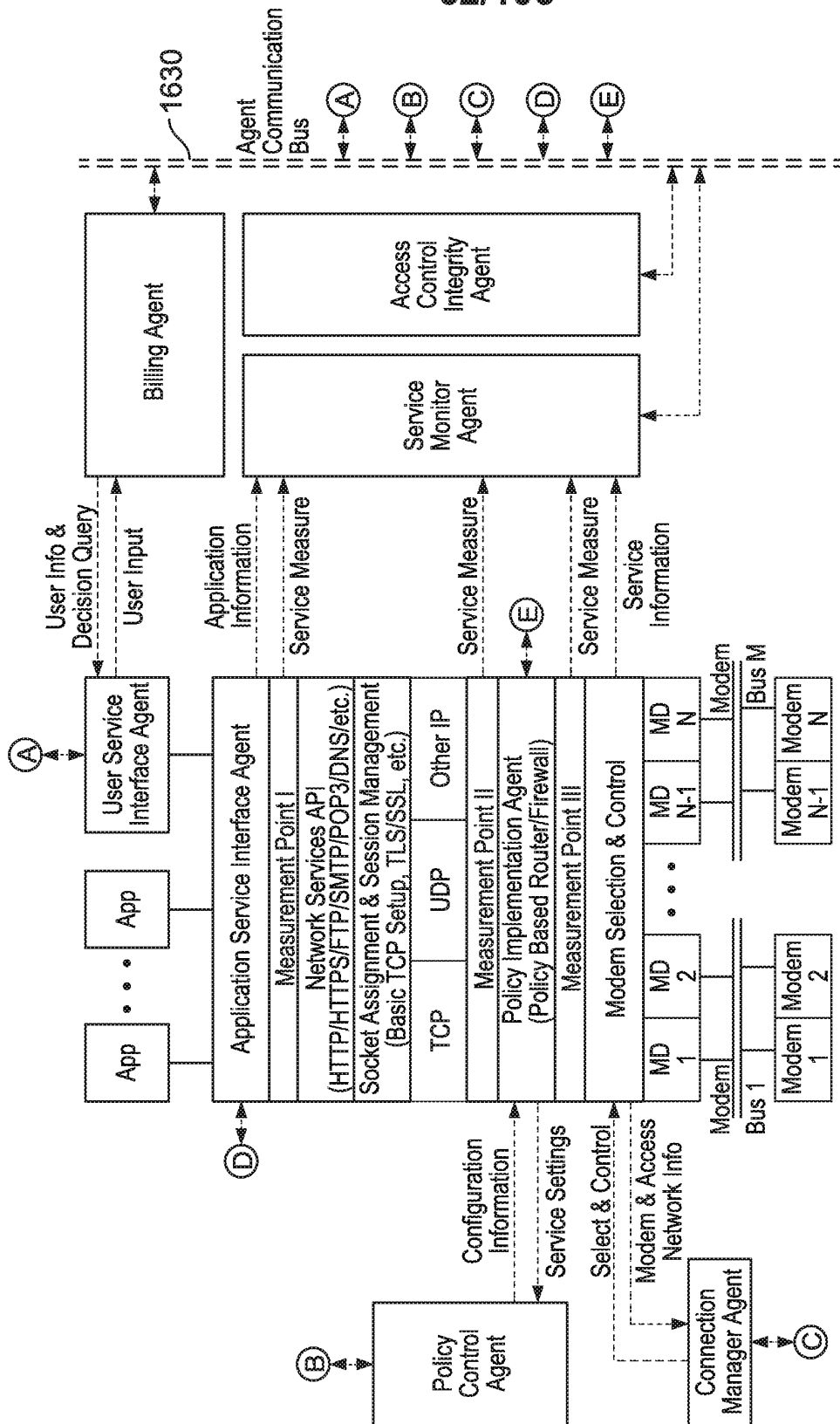


FIG. 33

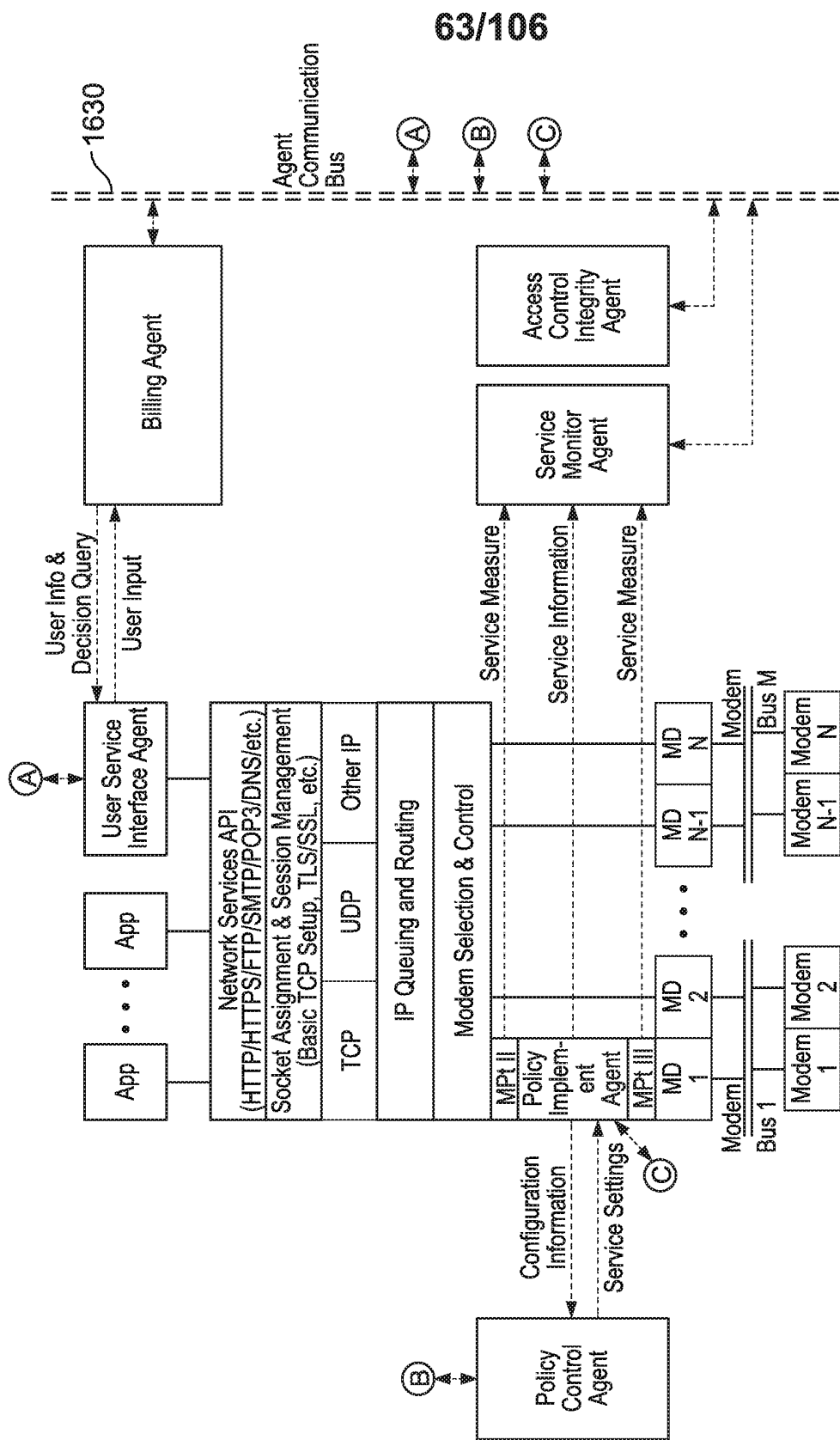


FIG. 34

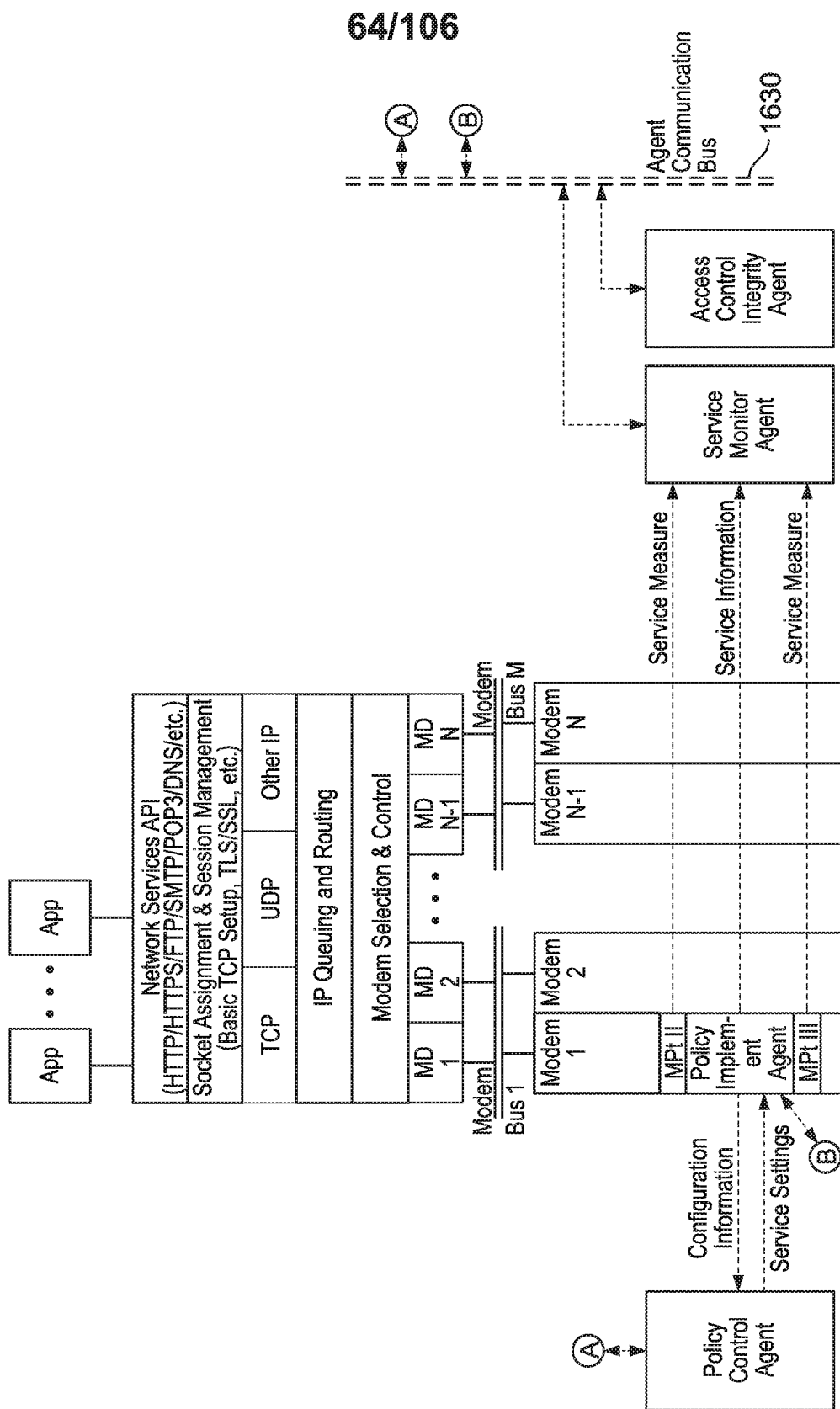
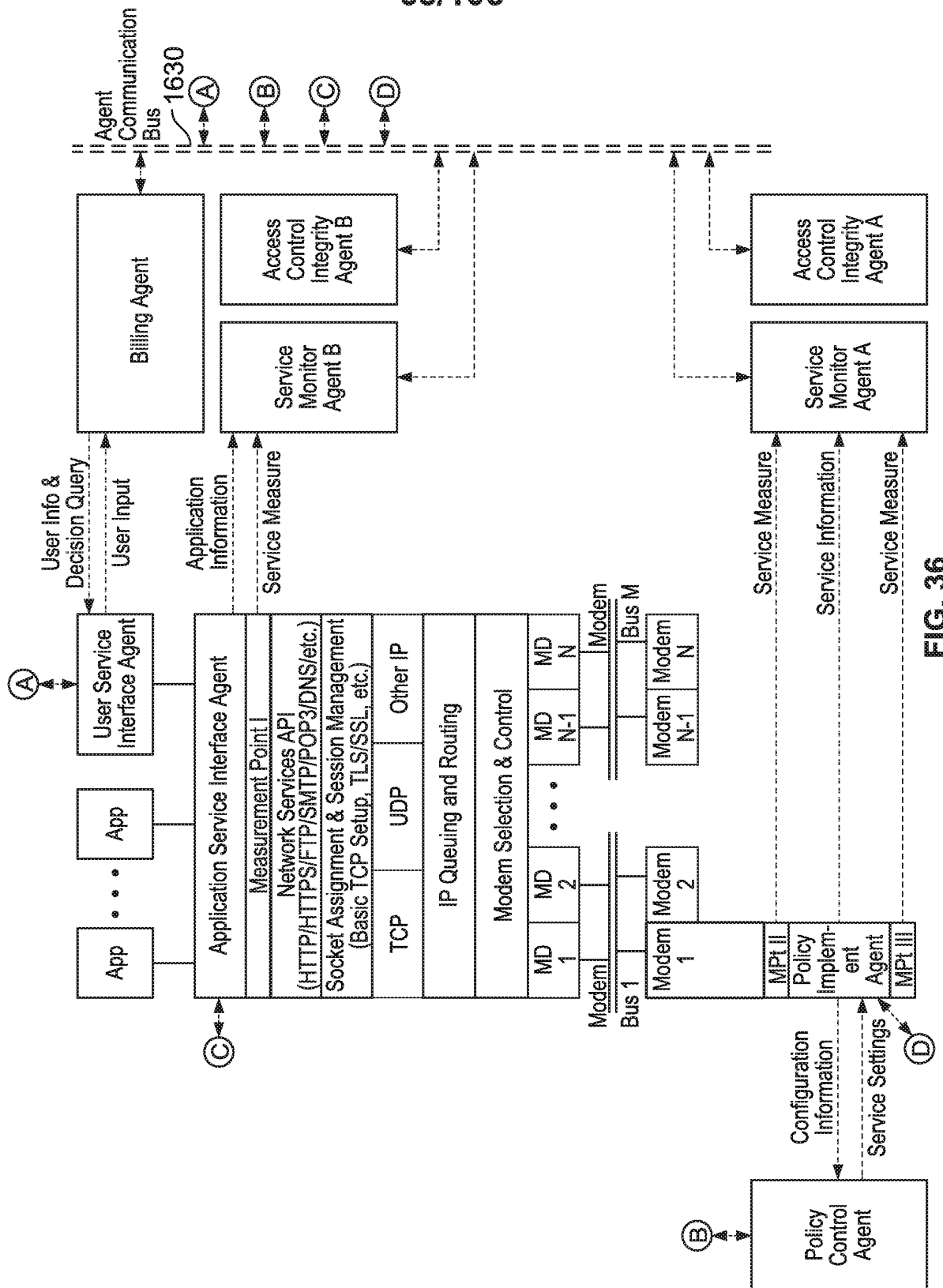
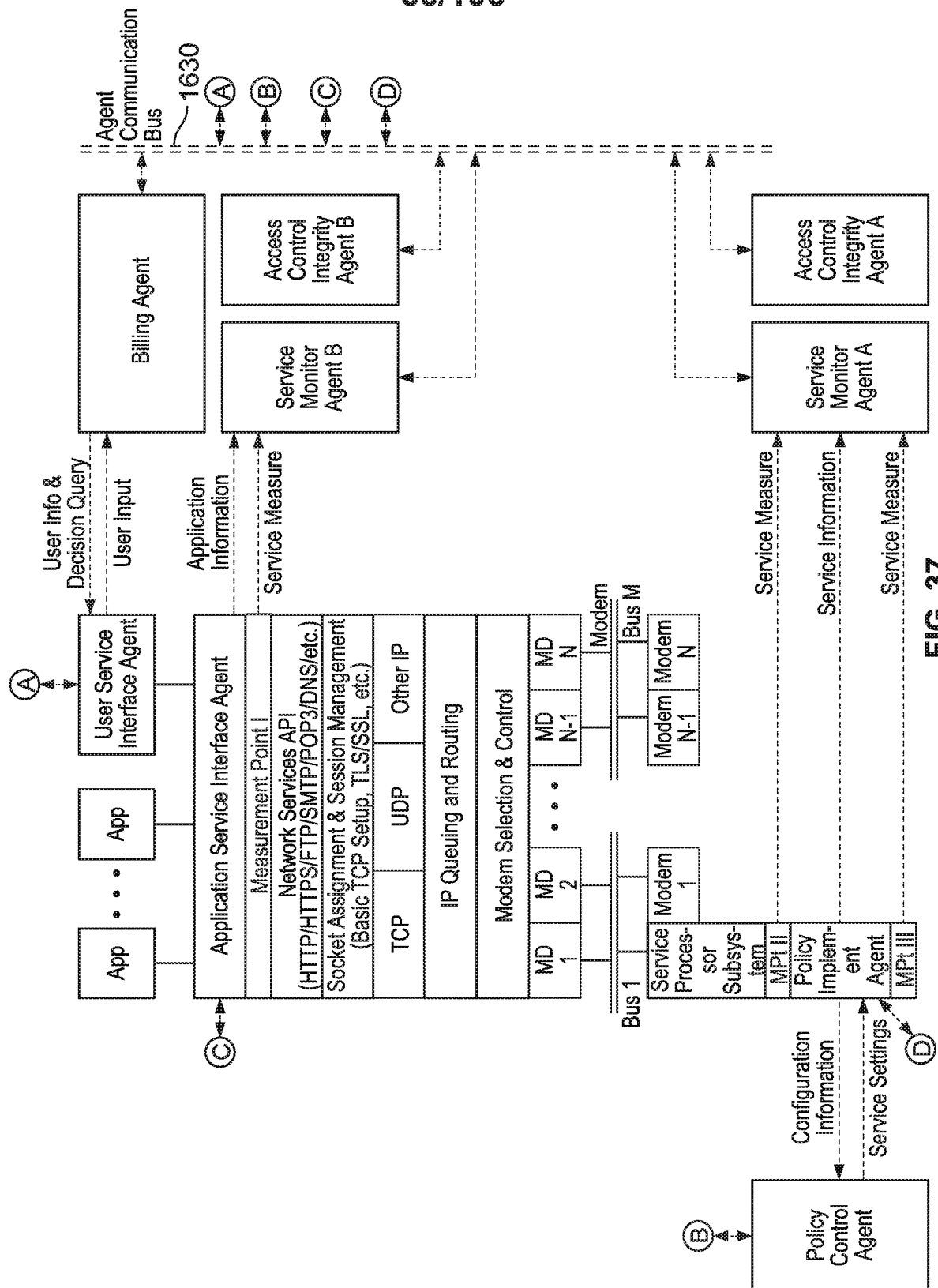


FIG. 35





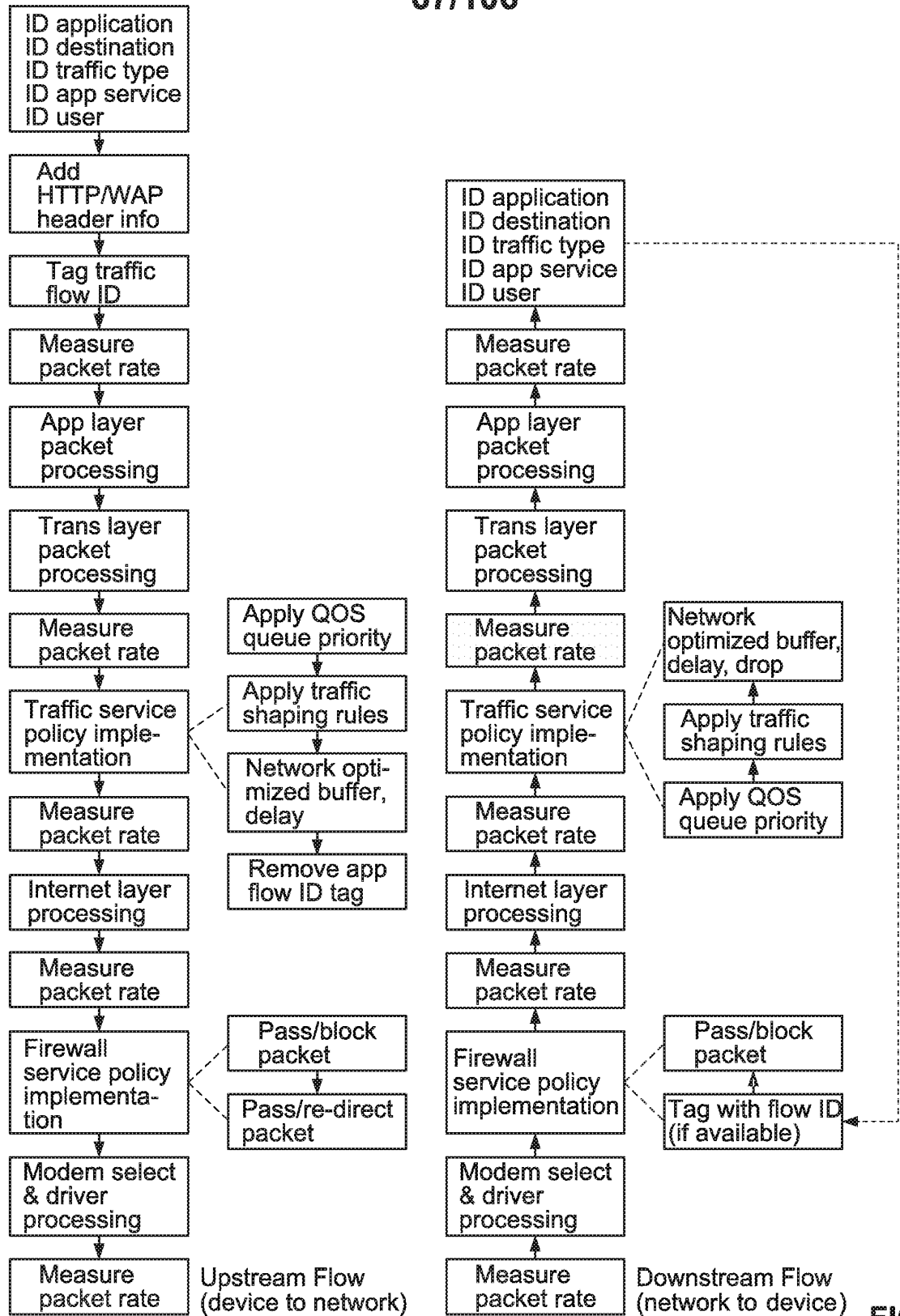


FIG. 38

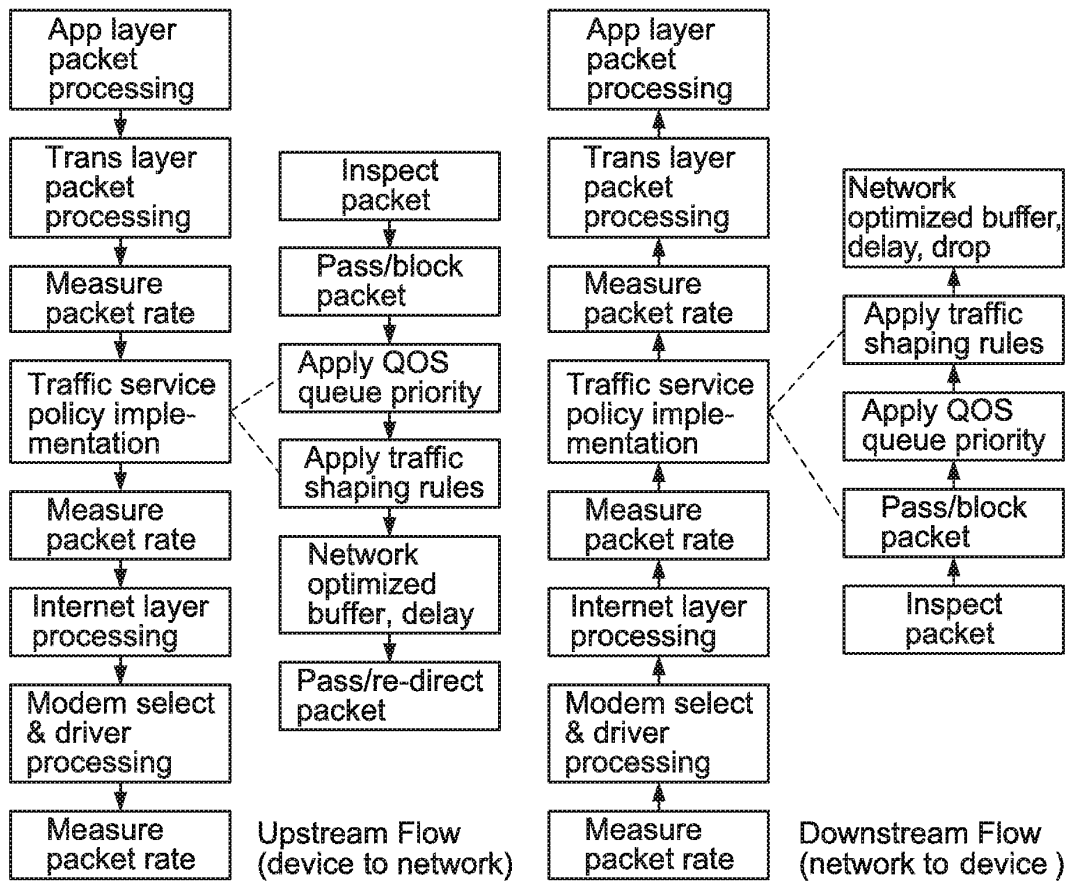


FIG. 39

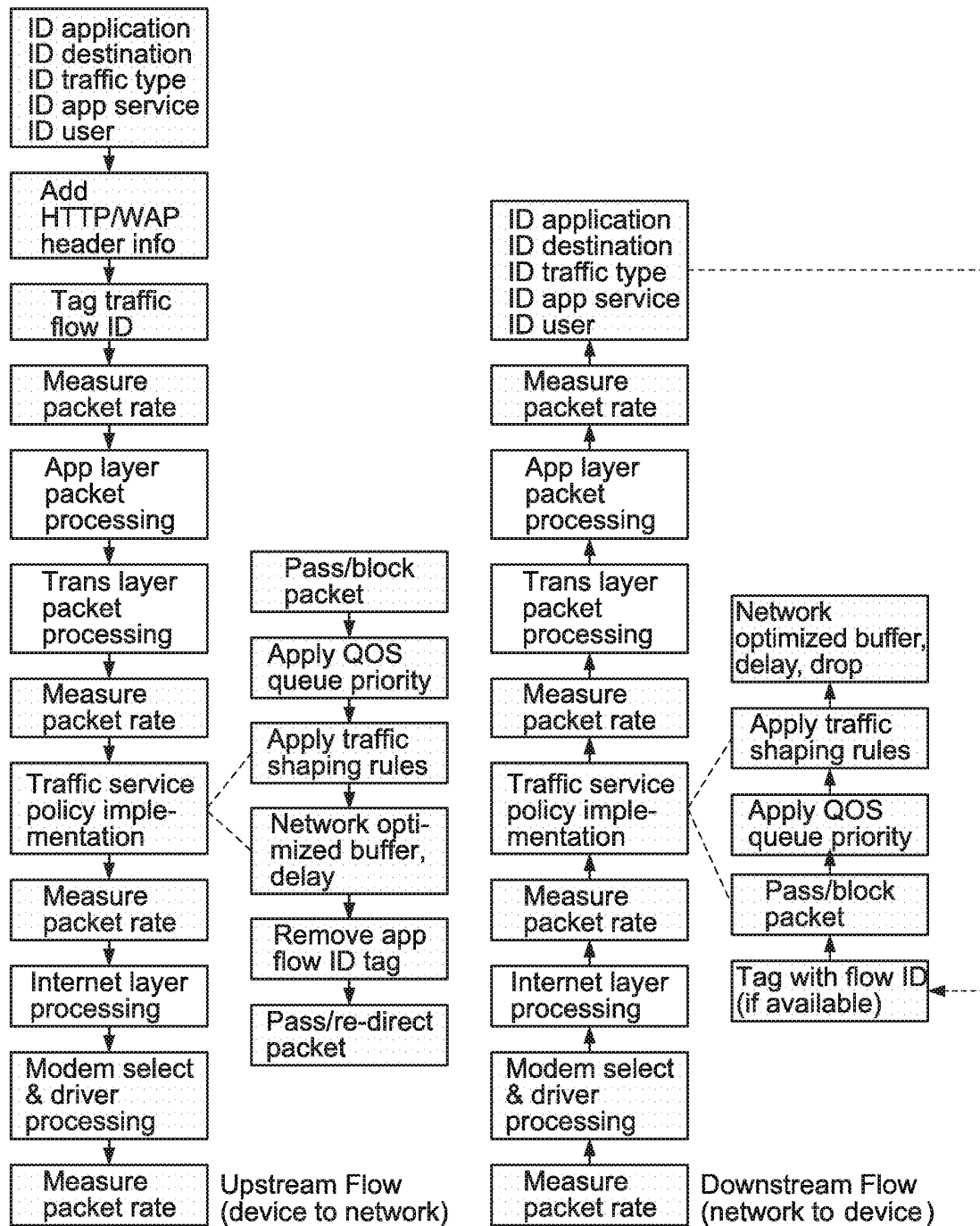


FIG. 40

Example Device CRM Data Collection and Reporting Classification	Partial Description	Example Sensitivity Level Classification	Example Authorization Level to Include in Report
Basic non-specific service usage parameters	User sensitive information is filtered from this report which is used for purposes such as service control, service control integrity monitoring or network traffic analysis.	Low	None
Service billing events or service plan selection events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with basic service agreement or enterprise agreement
Transaction billing events	Documents user selection process from service plan selection or billing options.	Low	Customer authorization with central billing agreement or enterprise agreement
Device location – customer location based service assist	Reports customer location for the purpose of assisting with location based services such as directions, yellow pages, shopping and social networking.	High	Customer authorization with basic service agreement or enterprise agreement
Device location – device or people tracking	Reports customer location for the purpose of providing tracking services for the device or the user.	High	Customer authorization with separate device tracking service agreement or enterprise agreement
Transaction associated information	Reports customer information such as networking activity, location, advertising usage, shopping behavior that is associated with a commerce transaction or happens around the same time as the transaction.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
URL history	Reports customer web surfing history.	High	Customer authorization – potential service discount or upgrade or enterprise agreement
Served and visited advertisement history	Reports the advertisements served to the user or which advertisements the user responded to. This information may be used to determine customer preferences or for a revenue sharing relationship with the advertisers.	Medium	Customer authorization – potential service discount, perk or upgrade or enterprise agreement
911 Service usage and location trace log	This log contains all information pertinent to emergency service personnel responding to a 911 call or other emergency situation. In some embodiments this information is password protected and generally not available to the service provider unless it happens to also be contained in reports authorized by the consumer as in the examples above.	Very High	Available only for 911 support or enterprise agreement

FIG. 41

Partial List of Example Service Policy Functionality Embodiments	Partial Description of Functionality Example	Example Authorization Level Required to Implement Embodiment
Block Downstream or upstream traffic	Various embodiments block traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Basic authority to pass or block traffic for access control, authorization, ambient services, or plan specific services typically may be provided by the user when they acknowledge the service plan agreement. Authorization to block traffic access as part of controlling user service costs typically may be provided by the service plan agreement options the user chooses to manage cost or may be provided when the user acknowledges the limitations in the UI notifications.
Pass downstream or upstream traffic	Various embodiments allow traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of command usage are access control prior to authorization, access control policy limits as defined by service plan or special device type, access control for ambient activation services, access control for error handling or access control for tamper prevention. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Same as above.
Limit maximum data rate	Various embodiments limit maximum data rate for traffic associated with one or more of user, network address identifier, application, content or data type, type of network, central provider, transaction provider, or transaction type. Typical but non-exhaustive examples of how this command can be implemented include limiting data rate to the device according to service plan; limiting data rate by network address identifier, application or content type for the purpose of implementing a tiered garden; limiting data rate in to different levels according to the type of access technology used by the present network connection; limiting data rate to different levels according to the service provider for the present network; or limiting data rate according to an agreement or lack of agreement with a transaction provider. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

FIG. 42A

Analyze traffic	Provides capability resident on the device to analyze device or user traffic statistics to determine how to implement adaptive policy control or how best to assist the user with notification messages. In some embodiments it is important to perform traffic analysis locally on the device to reduce network chatter with the Control Processor or to maintain user CRM privacy levels by not sharing sensitive raw traffic usage history needed to determine implementation of less sensitive service control policies. Typical but non-exhaustive examples of command usage are analyzing traffic usage statistics or patterns to determine compliance with service plan limits; analyzing traffic usage statistics or patterns to determine likely future compliance with service plan limits; analyzing traffic statistics or patterns to categorize usage according to network address identifiers, applications, content types, network types or central providers; analyzing traffic demand vs. usage statistics or patterns to determine if user may be better served with another service plan; analyzing traffic statistics or patterns to identify potential tamper threats. This command may be implemented in instantaneous policy implementation mode or adaptive policy control mode, but adaptive application of the analysis results is typically associated with adaptive policy control mode.	Authorization to analyze traffic for local device service policy control purposes or 911 service typically may be provided for in the basic service contract. Authorization to transmit a complete or filtered version of the traffic analysis to the Service Controller typically may be provided under user selected options in the service plan contract.
Successive limitation	Provides capability to begin with one limit on access or data rate according to a set of defined service usage trigger criteria, to further limit access or data rate according to said criteria, and then to successively remove limits according to said criteria. In some embodiments this function provides for service usage that starts at a given level for one or more service aspects, but as said service aspect exhibits usage that potentially threatens an overage on service plan limits then the level of service for said service aspect is reduced successively until the threat of service plan overage is reduced or eliminated. In some embodiments, the limits on service level for said service aspect are eventually removed either all at once or successively over a specified time period or set of time periods so that the limits on service level for said service aspect are eventually removed if the service aspect is used less vigorously for a period of time. In this type of embodiment the projection for future service usage by a given service aspect is assisted by the analyze traffic statistics function. As a more specific example, the service aspect may be a URL address that is popular with the user and demands a high service consumption, and the data rate allowed to that URL may start at a relatively high level when the user first begins to surf and as long as the surfing session is finished quickly there is never a reduction in service level, but if the user surfs for a longer time so that service usage begins to threaten plan limit overage, the data rate allowed to that URL is successively reduced the longer the surfing session occurs. Continuing this	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.

FIG. 42B

	<p>example embodiment, if the URL is not visited for a defined period of time then the data rate limitation may be removed in steps over multiple pre-defined time periods, or may be removed all at once back to the initial data rate established in the service policy for that URL. Other specific embodiment examples include email download or upload data rate; download or upload rates for certain types of file transfers; or download or upload rates for a given network access technology or central provider. This command is associated with adaptive policy control mode for the Service Processor. In more advanced adaptive embodiments, the policy control system first identifies those service aspects that are consuming a large percentage of the service usage and then begins to successively limit service level only for these highest usage service aspects so that all other service aspects that are not responsible for potential service plan limit overage continue to receive relatively high service levels. In another embodiment, some high usage service aspects may be exempt or partially exempt from limitations in service level, as for example a service aspect that is associated with a secondary source of service or transaction payment or that may be separately accounted for in the service plan usage reporting.</p>	
Limit email file transfers	<p>Sets and enforces limits on email downloads. In some embodiments this can include use of the successively limit functionality. In some embodiments, this is accomplished by identifying specific email downloads or uploads and controlling traffic for those traffic flows. In other embodiments, this includes interacting with the email application to set download or upload file settings. This functionality may be implemented in instantaneous policy implementation mode or adaptive policy control mode, with the more advanced functionality such as successive limitation on email file transfers being implemented in the adaptive policy control mode.</p>	<p>Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.</p>
Seek to manage below service limit	<p>Implements adaptive policy control in an attempt to manage service usage to reduce service plan limit overages. In some embodiments there are successive limits on service level for overall traffic, or for the highest usage service aspects, with the successive limits being lowered until average service usage is projected to be below service plan limits. The algorithms that may be applied to achieve this adaptive service level limitation are quite varied and only a few are given here. In one embodiment, the service usage for the service plan period is projected using the analyze traffic functionality, and overall device data rate is successively limited until service usage is projected to be below the service plan limit. In another</p>	<p>Same as above.</p>

FIG. 42C

	embodiment, the analyze traffic functionality is used to identify those service aspects that are causing the majority of the service plan usage, and then each of those service plan aspects are limited using the successive limitation functionality, with the service level limitations being based on the traffic usage patterns and specific application scenarios for each service aspect. For example, in some embodiments the service aspects that are creating the most service usage are subjected to more service level limitation than service aspects that are creating less service usage. Service usage may be defined as usage of a raw service measurement such as total data consumption, files downloaded or time spent on network, or it may be translated into an economic measure using the lookup service cost functionality. In some embodiments, the period of time elapsed in the service accounting period is taken into account in determining...	
Synchronize service usage counters	Synchronizes service usage counters on device from time to time to minimize service accounting errors between the device data base and the central billing data base. In some embodiments this is a part of the Service Processor heartbeat communication system that need not happen every heartbeat. In some embodiments this occurs with a request for update by the device to the central billing system or to a server function in the Service Processor	Provided for in the basic service agreement.
Lookup service cost	Provides a data base of service usage vs. cost for each type of service offered on the device. Provides for a lookup function of service cost.	Same as above.
Convert service usage to service cost	Uses the service cost vs. usage lookup function to transform one or more service usage aspects to one or more service cost aspect. One example embodiment provides a service cost measure for one specific aspect of service usage, for example total data consumed over a period of time. Another example embodiment provides a total service cost measure for all service usage over a period of time.	Same as above.
Notify user of service overage	Sends a notification message or screen to the UI to inform the user that the one or more aspects of service usage has exceeded the specified limits of one or more service plans. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Same as above.
Project service usage	Uses the analyze traffic functionality and projects an estimate of what the traffic usage will be at the end of a service plan measurement interval if the service usage does not change. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above

FIG. 42D

Notify user of service cost overage	Performs a service cost estimate based on one or more aspects of service usage and informs the user that the one or more aspects of service cost has exceeded the specified limits of a service plan. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen.	Provided for in the basic service agreement.
Notify user of usage behavior likely to run over service usage limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, notifies the user if the projected usage is over the service plan limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected service usage is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Notify user of usage behavior likely to run over cost limit	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user if the projected cost is over the service plan cost associated with the service plan service limit for the service plan measurement interval. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.
Project user service cost if usage behavior continues	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, uses convert service measure to service cost functionality to estimate the service cost of the projected service overage, notifies the user of what the projected cost will be if the service usage behavior remains the same. In some embodiments, the user notice is a pop-up window and in some embodiments there is a continuous display on a small gauge in main screen. In some embodiments the projected cost is made based on assuming the average service usage per unit time in the present service plan measurement interval does not change for the remainder of the service plan measurement interval.	Same as above.

FIG. 42E

Limit access likely to cause overage and notify	Uses the project service usage functionality to determine if the service usage is projected to go beyond the service plan limit, if the service usage is projected to go over the service limit, notifies the user that limits are being applied to keep service usage or cost under the service limit, applies limits to various aspects of service usage to bring down usage so that projections are within service limits. In one embodiment, the seek to manage below service limit functionality is used.	Authorization to limit data rate for all traffic or a subset of traffic typically may be provided in the options the user specifies for how to limit potential or actual service plan usage or cost overages. For example, one user may choose to have no limits and be notified when service usage is over or about to go over, while another user may choose to allow traffic control sufficient to keep service usage under the service plan limit without any notification.
Require acknowledgment of notification	Requires the user to acknowledge a notification of potential service or cost overage or a notification of an option to limit the service overage or cost of service overage.	Provided for in the basic service agreement.
Log or report acknowledgment of notification	In some embodiments, the user acknowledgment of notification is stored, or sent to the Service Controller, or stored and later sent to the Service Controller.	Same as above.
Notify user of service plan options prior to running over service usage limit	Notifies the user of options to extend the service plan limit before reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Notify user of service plan options after running over service usage limit	Notifies the user of options to extend the service plan limit after reaching the service plan limit. In some embodiments, accepts user input on which service plan extension option if any the user wishes to accept. In some embodiments, notifies the billing system when the user has accepted a service plan extension option.	Same as above.
Time of day variations	Each of the functionalities for traffic control, service cost, service limits may be modified with a time of day variation so that the values used are different for different times of day.	Same as above.

FIG. 42F

Access control enable list	List of service usage activities that are enabled.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the control data base.
Access control block list	List of service usage activities that are blocked.	Same as above.
User service control option UI	Provides the user with a list of options for how they would like to control service usage or service cost.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.
User service notification option preference	Provides the user with a list of options for how they would like service notification information to be displayed. In some embodiments provides the user with the option to turn off one or more aspects of service notification. In some embodiments the user is not allowed to turn off notification for service usage events that require user decision or acknowledgement.	In some embodiments UI screens and scripts are defined by the UI agent software version and access to modifying this software is restricted to service controller, VSP or other network function with proper credentials to access the UI data base. Some embodiments call for the UI screens or UI screen content to be generated by the service controller, VSP or another network function (e.g. service usage notification gateway or billing system) and in this case access is restricted to service controller, VSP or other network function with proper credentials to access the UI pass through screens.

FIG. 42G

User CRM or service usage monitoring filtering option preference	Filters the device and/or user information that is being collected before it is reported to the network to maintain the desired level of user privacy. In some embodiments the user defines preferences on user privacy that are used to define the filter settings.	In some embodiments this is not accessible by the network and only may be modified by the user. In other embodiments it may be read but not written by the network and in this case authorization is restricted to service controller, VSP or other network function with proper credentials to access the filter settings data base. In some embodiments the network is allowed to change the CRM filter settings and in this case Authorization restricted to service controller, VSP or other network function with proper credentials to access the CRM filter settings data base.
Service usage billing event record	A record of service usage billing events. In some embodiments this record is transmitted to the billing server or another network function to aid service billing or billing reconciliation.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Bill by account	The bill by account embodiments provide for service billing to accounts different than the main user account, for example tracking network device chatter that is not desired to be billed to the user, transaction partner access costs that are shared with or billed to the transaction partner, ambient service cost tracking, tracking temporary account costs, etc.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Central billing transaction and event recording	Billing event tracking and reporting associated with the central provider open billing embodiments. Some embodiments include generation of billing certificates or receipts. In some embodiments the device may serve as a billing feed.	In some embodiments authorization restricted to service controller, VSP or other network function with proper credentials to access the billing data base. In some embodiments the user is allowed to read but not write the data base.
Service owner registration or re-registration	Function that allows a portion of the device credentials to be programmed to indicated the VSP.	In some embodiments authorization to write the device is restricted with security signatures or other security methods to the VSP and possibly the central provider. Some embodiments involve provisions to report to a network function when the VSP settings are changed or the software is uninstalled. Other embodiments involve restoring VSP settings or software if removed.

FIG. 42H

Credentials swap	Function that provides for swapping of credentials, for example temporary credentials to permanent credentials.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the credentials data base.
Account information swap	Function that provides for swapping the account information, for example temporary account to permanent account.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the activation service profile data base.
Configure or re-configure service processor for new device service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Ambient service profile definition	Function that provides for service processor programming for all the information that defines the ambient service profile, device credentials, VSP and other necessary parameters.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the ambient service profile data base.
Analyze service usage statistics	VSP function to analyzer service usage statistics for a device, defined group of devices, defined group of service plans or service profiles, defined group of users or other groupings.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Dry lab test new service policy	Allows simulated testing of draft service profiles and/or service plans against device usage statistics for a defined group of devices or users or service profiles, or against simulated device service usage behavior. Some embodiments show the estimated profitability of proposed service profile and service plan. Some embodiments allow decomposition of the service usage statistics to identify the user group service usage activities that may be modified by changing the service usage control policies or made more profitable by changing the service plan billing policies.	Authorization typically restricted to service controller, VSP or other network entity with the credentials to access the service usage history data bases.
Beta test publishing system	Function that provides for service processor programming for all the information that defines the service profile device credentials, VSP and other necessary parameters for a beta test device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.
Publish new service	Function that provides for service processor programming for all the information that defines the service profile, device credentials, VSP and other necessary parameters for a production device group.	Authorization restricted to service controller, VSP or other network function with proper credentials to access the service profile data base.

FIG. 42I

Roaming selection service	Function that surveys available roaming service partners, looks up the billing rates for the partners, and displays to the user the set of choices and billing rates. In some embodiments the roaming partner billing rates for one or more roaming partners are applied to a typical user service usage scenario for the purpose of estimating possible projected roaming costs and displaying those costs to the user. In some embodiments the roaming data is stored locally on the device and periodically updated with network refreshes, while in other embodiments the data base is looked up at the time of service. In some embodiments, the user is asked if they would like to modify their service usage notification or control profiles to save roaming costs and if the user responds yes they are provided with a set of options for changing service usage notification or service usage control policies.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the roaming service.
Roaming usage count	Provides a service usage estimate to the user while roaming.	Same as above.
Roaming cost service	Provides a service cost estimate to the user while roaming.	Same as above.
Roaming policy control service	Provides the user or VSP with the capability to switch service usage notification or service usage control policies while roaming. Some embodiments provide for restrictions to roaming carrier options. Some embodiments provide policies based on carrier chosen. Some embodiments provide policies based on the service cost for carrier chosen. Some embodiments specify preferred roaming lists that may be different than the central provider roaming list.	Same as above.
Switch policies for new network	Provides the user or VSP with the capability to switch service usage notification or service usage control policies depending on which network the device is connected to. Some embodiments provide for restrictions to certain network options. Some embodiments provide policies based on network chosen. Some embodiments provide policies based on the service cost for network chosen. Some embodiments provide for a network connection preference list.	Authorization to modify the policies typically restricted to the VSP or other entity responsible for managing the network selection policies.

FIG. 42J

Service
Processor
Authorization

81/106

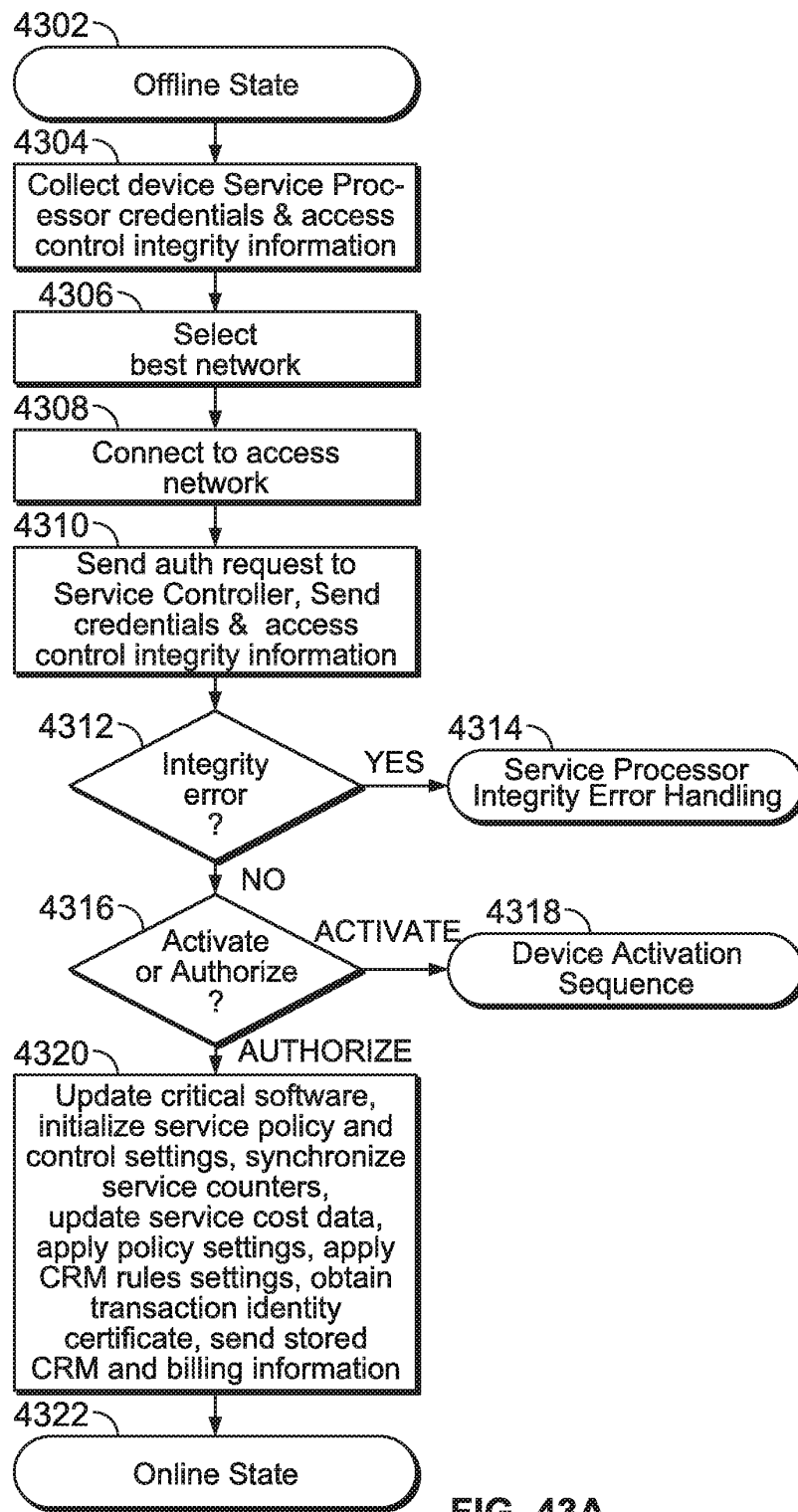


FIG. 43A

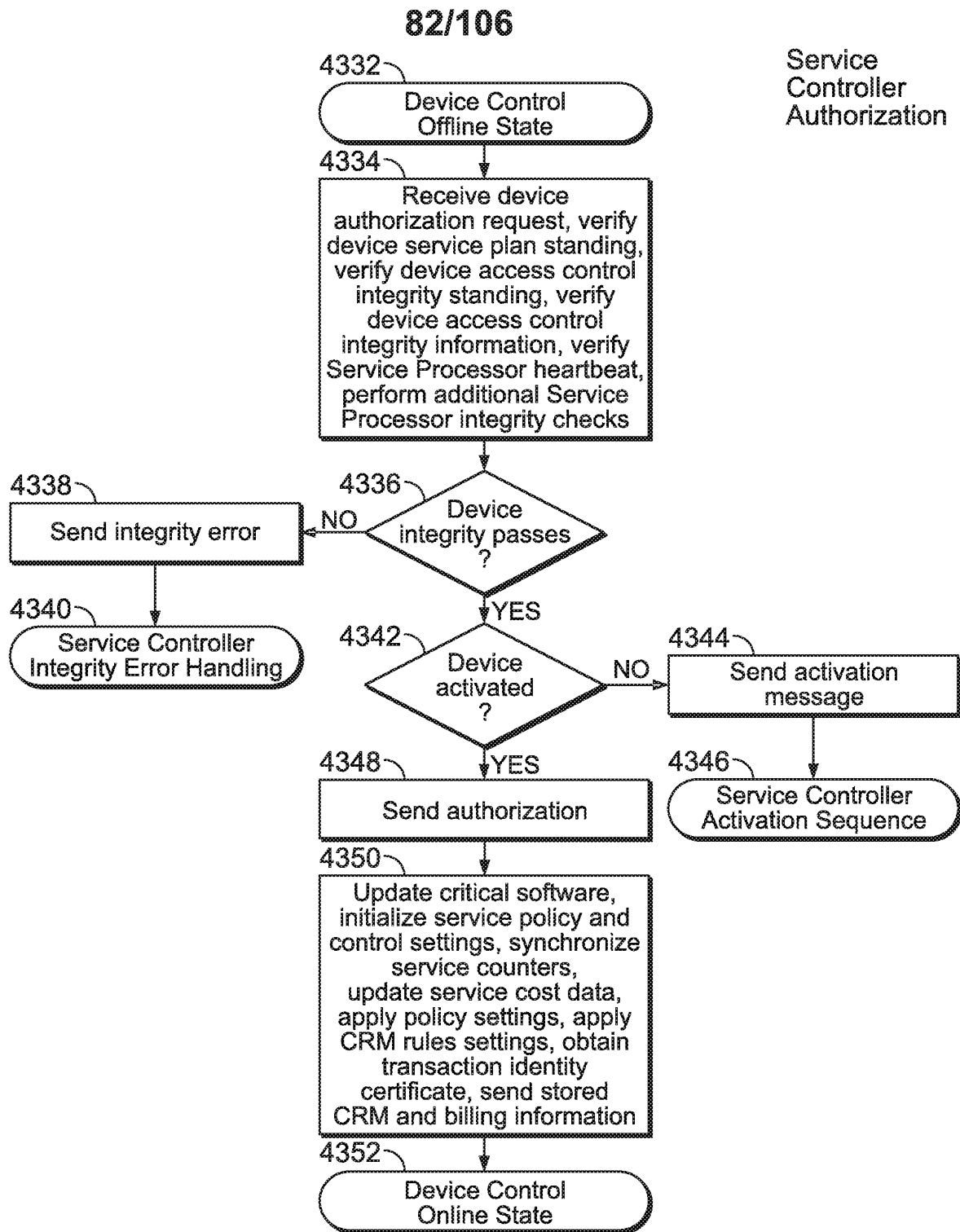


FIG. 43B

83/106

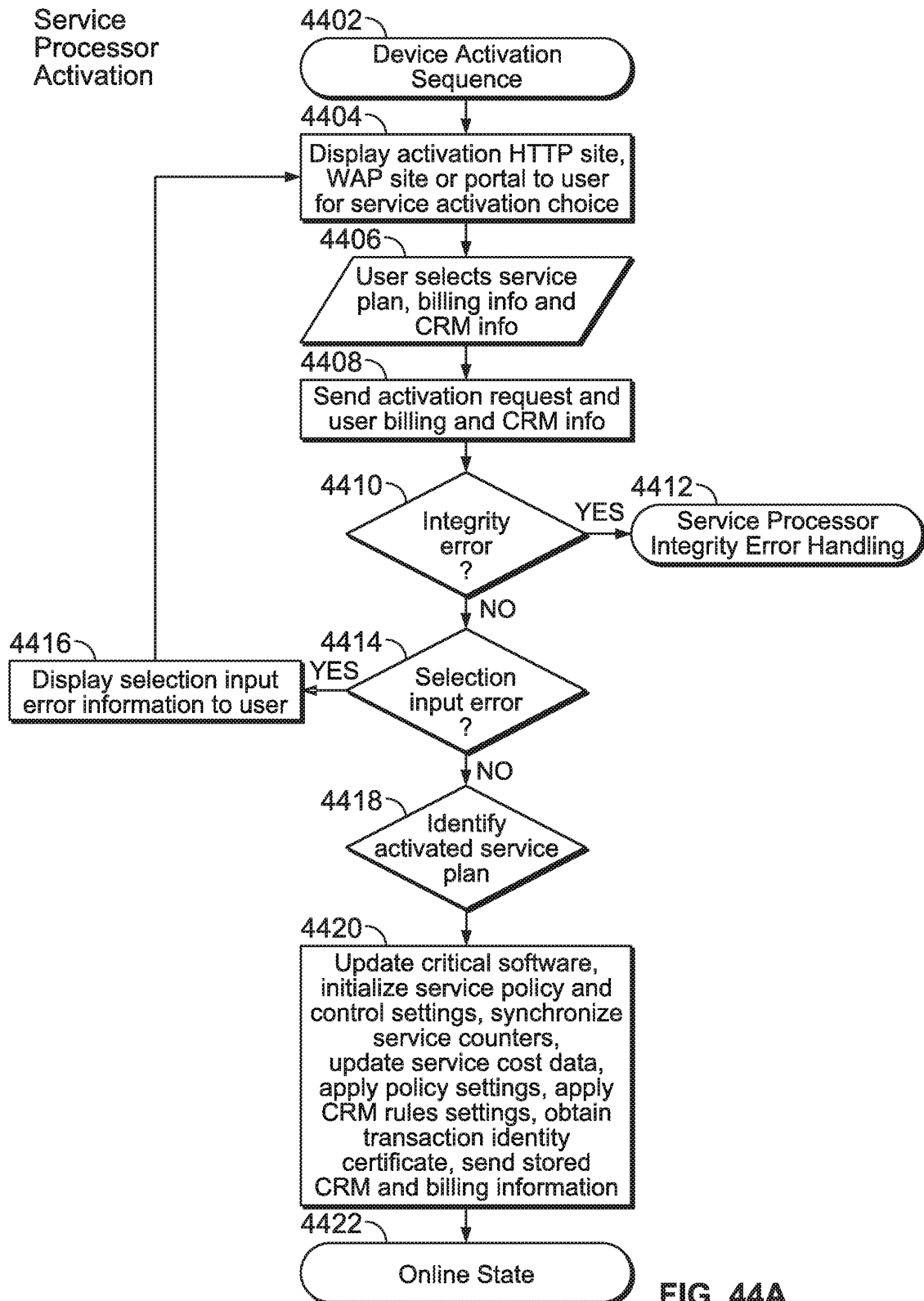


FIG. 44A

84/106

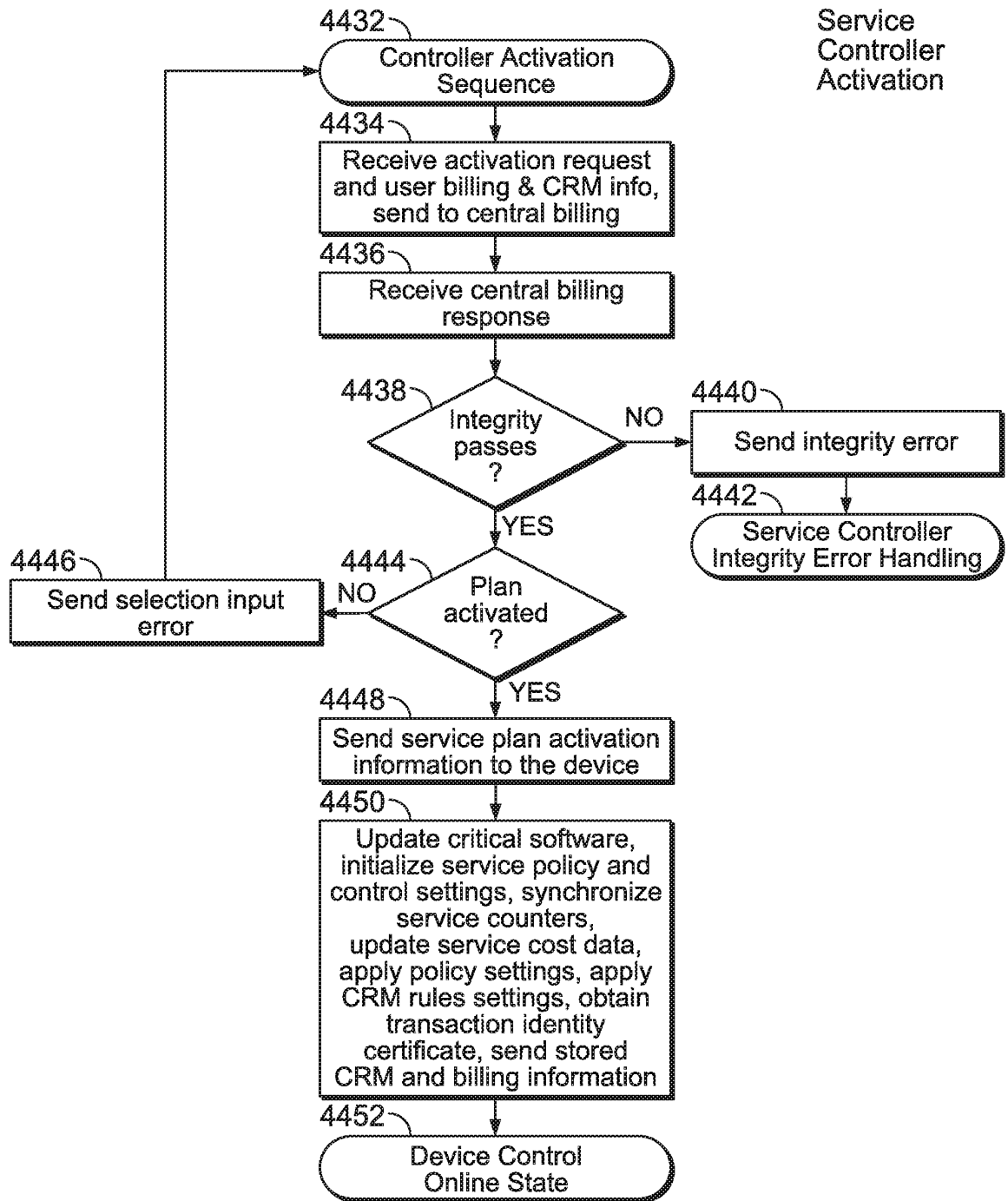


FIG. 44B

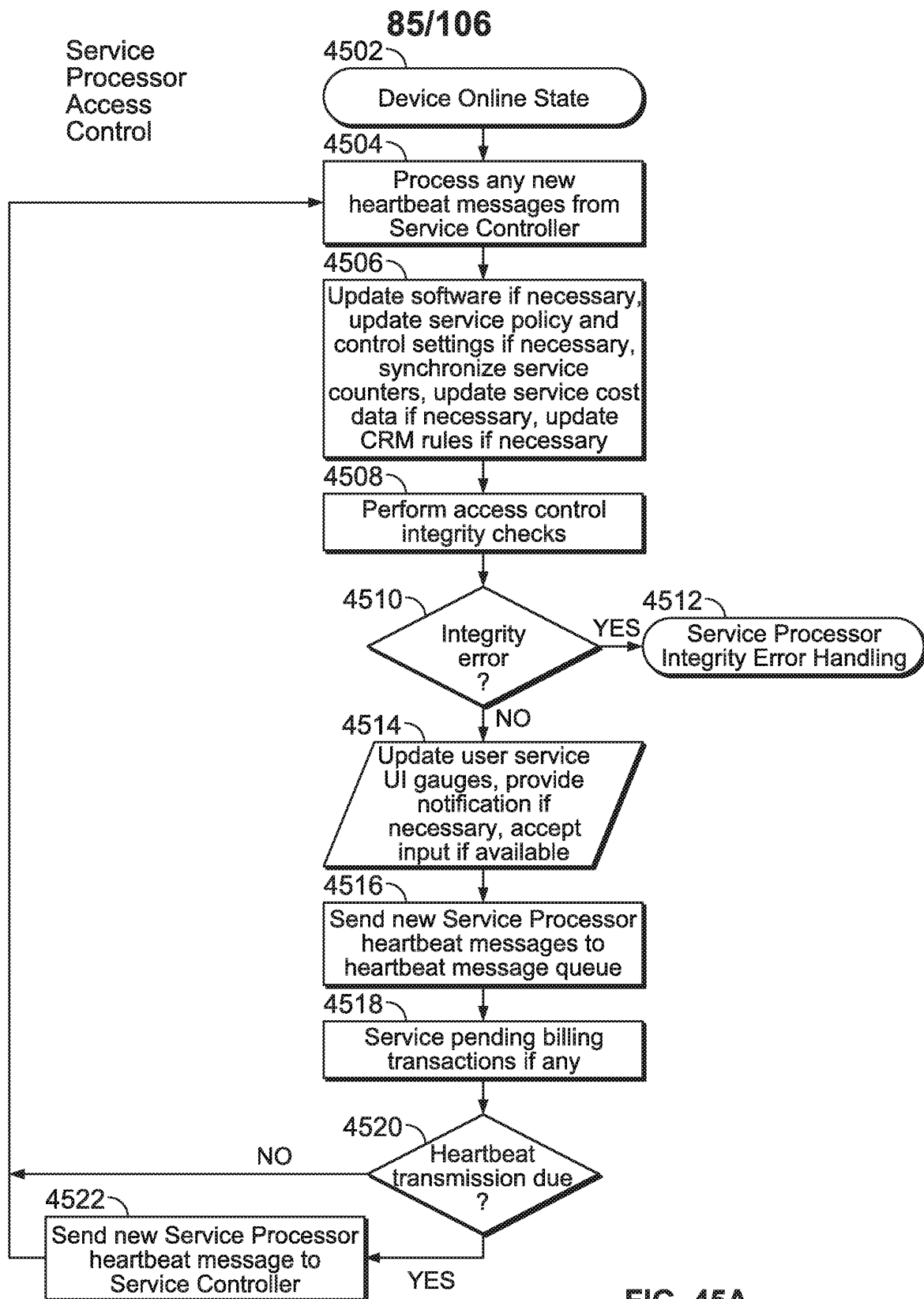


FIG. 45A

86/106

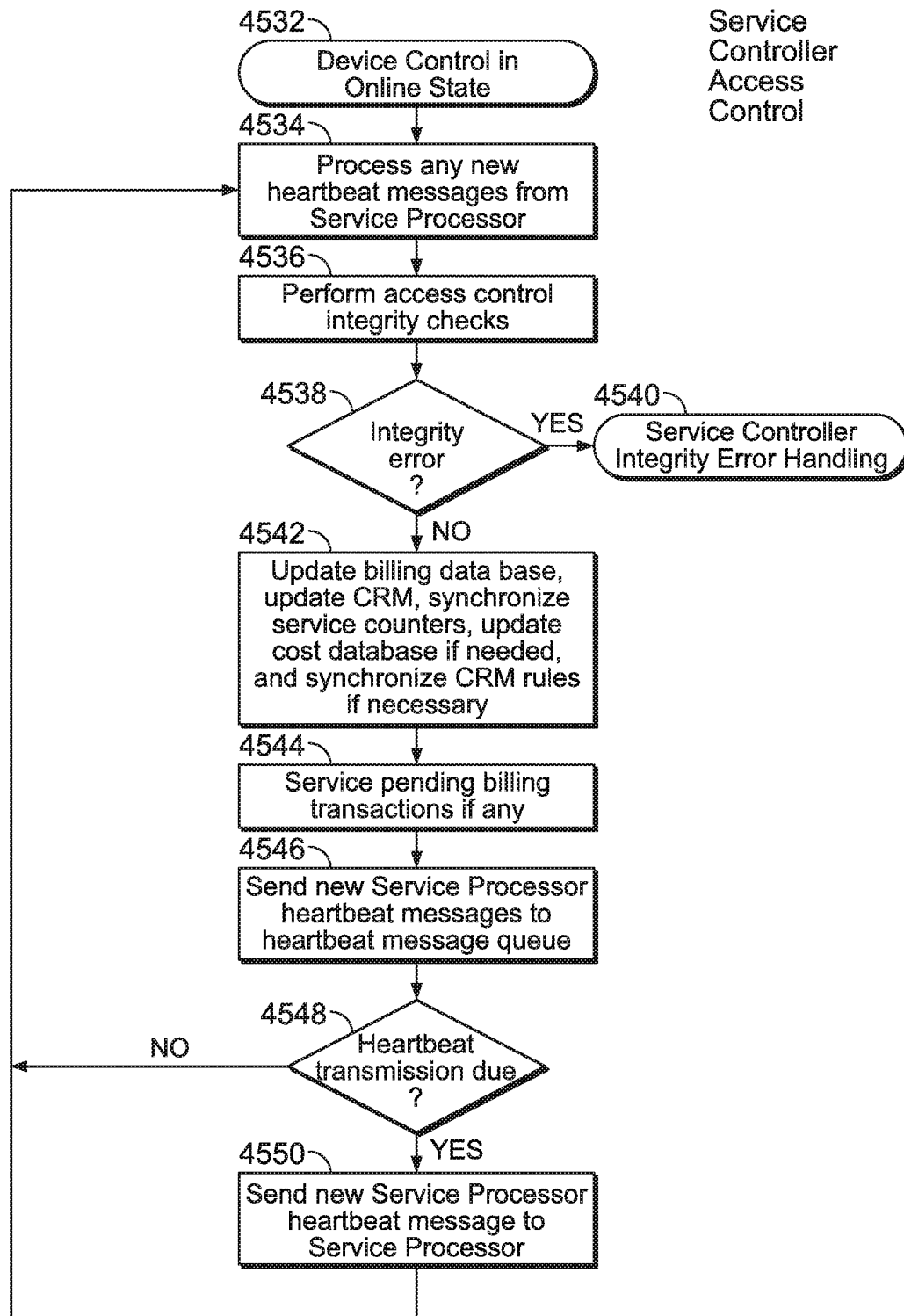
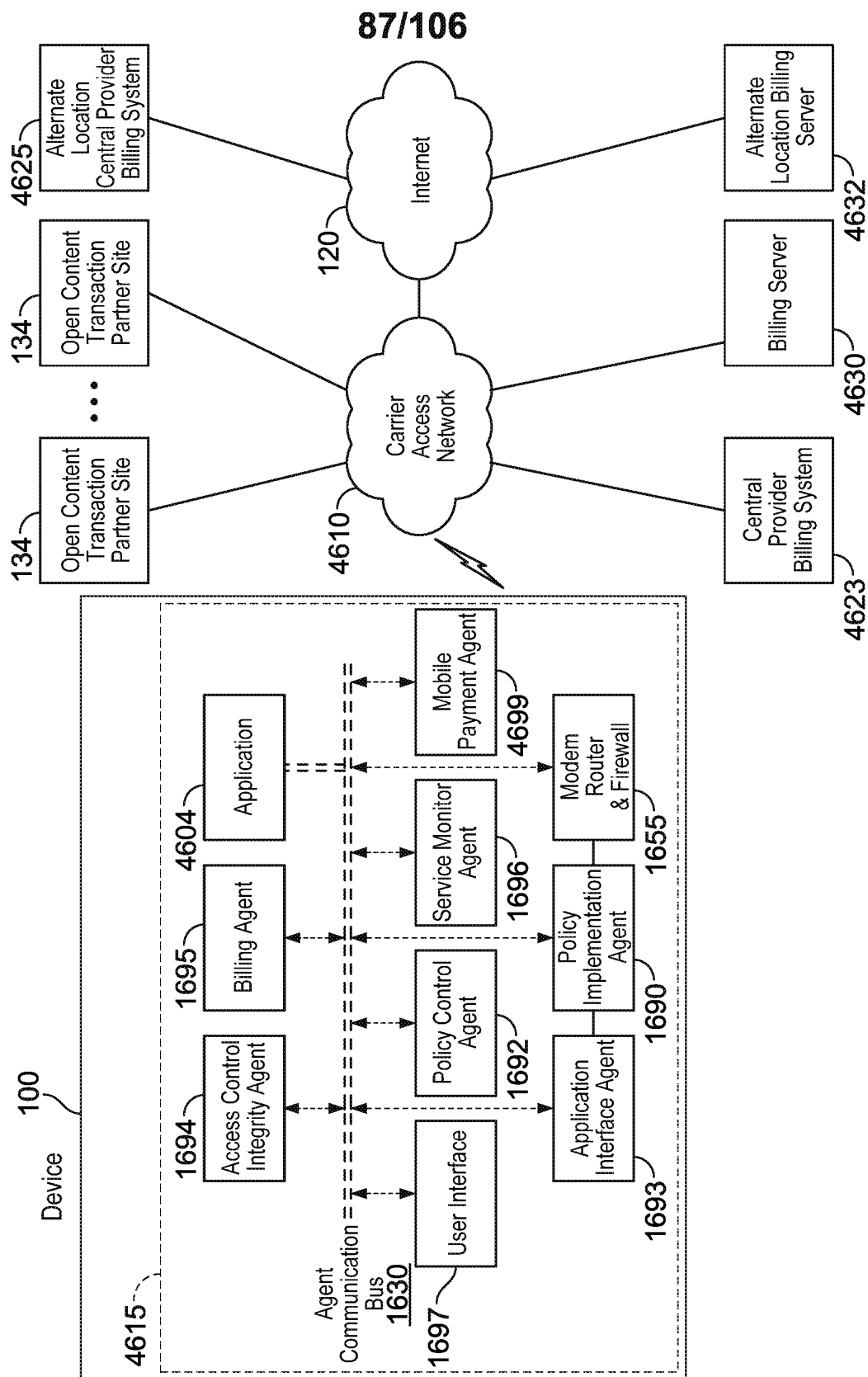


FIG. 45B



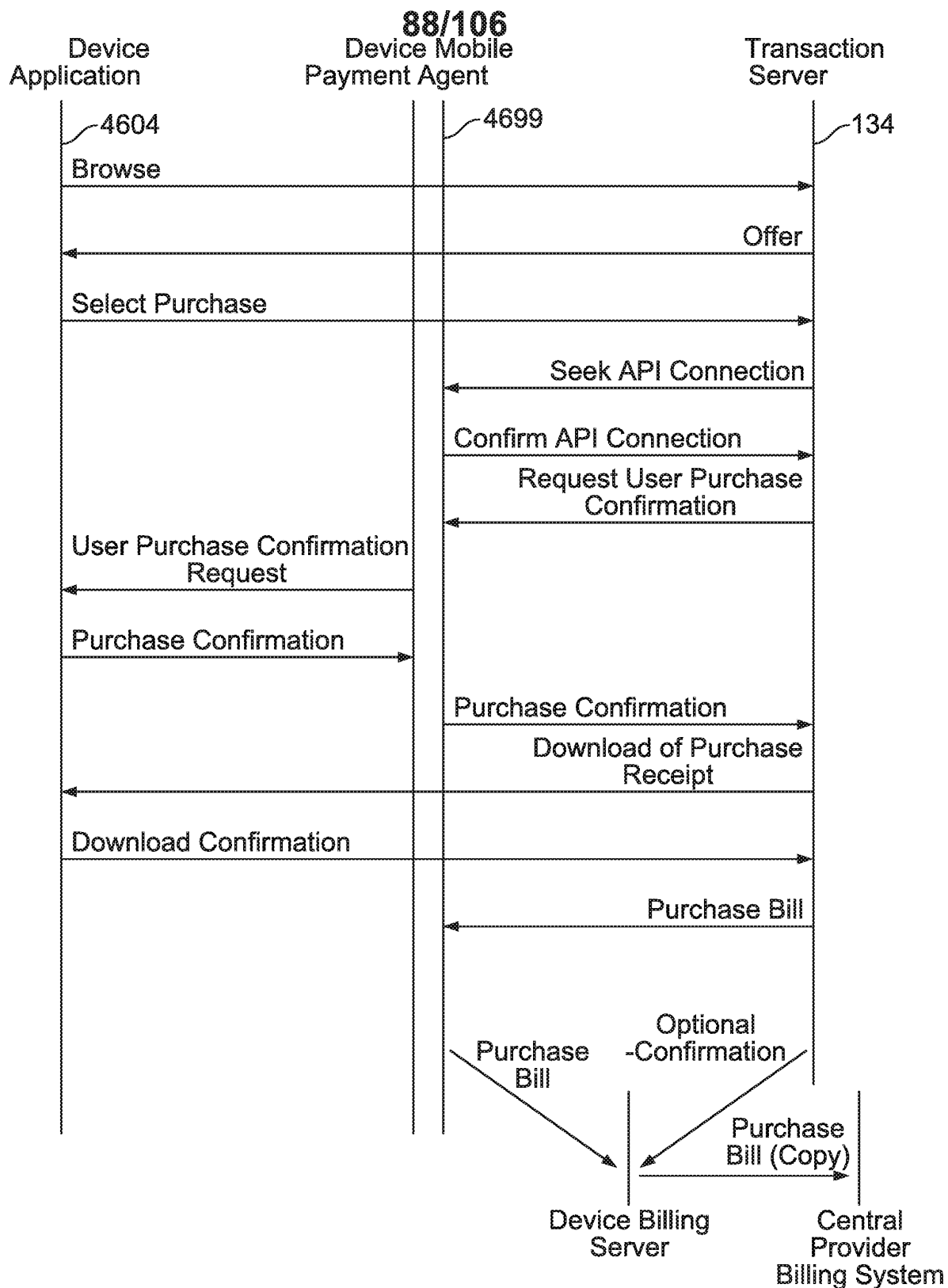


FIG. 47A

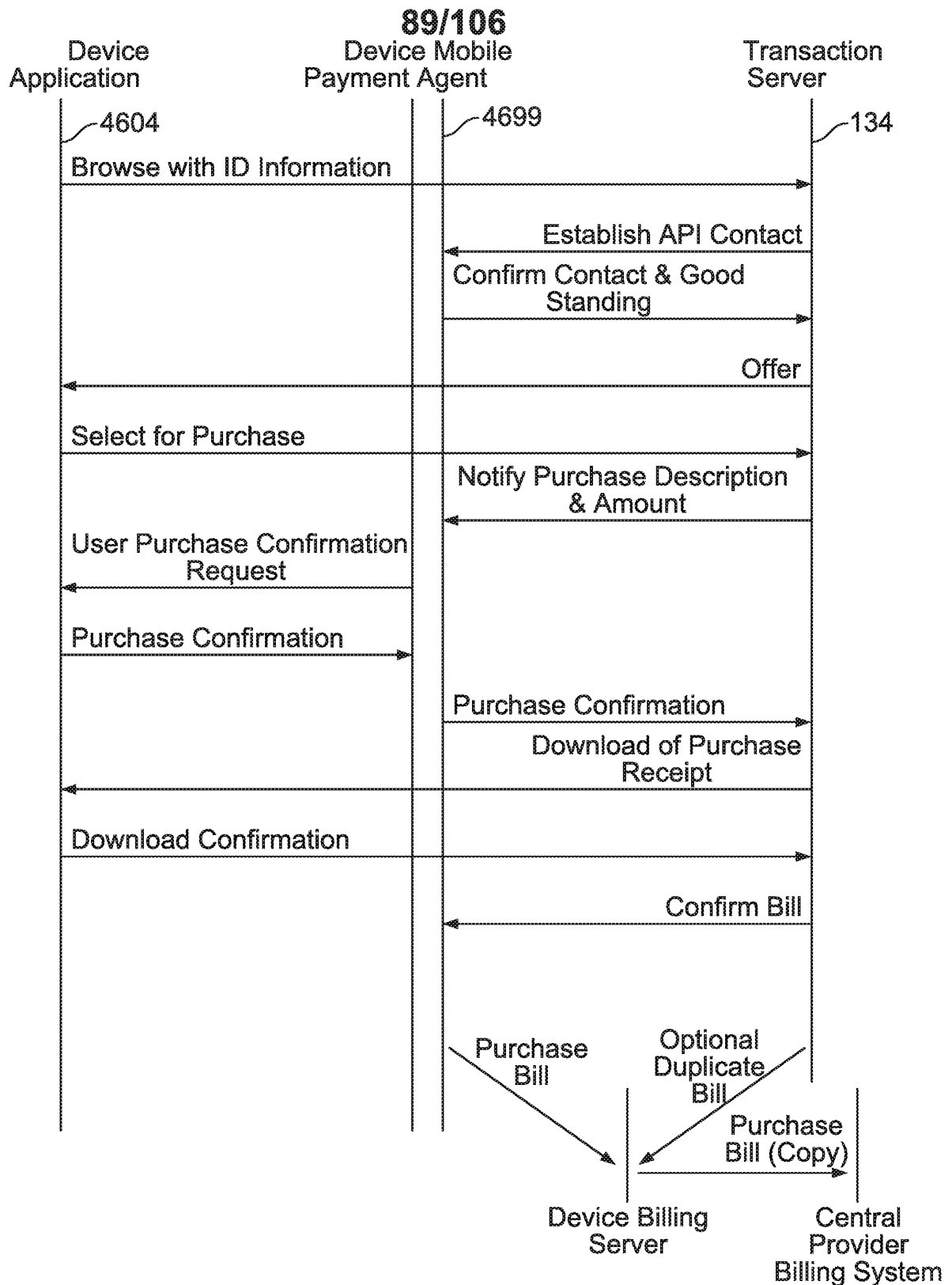


FIG. 47B

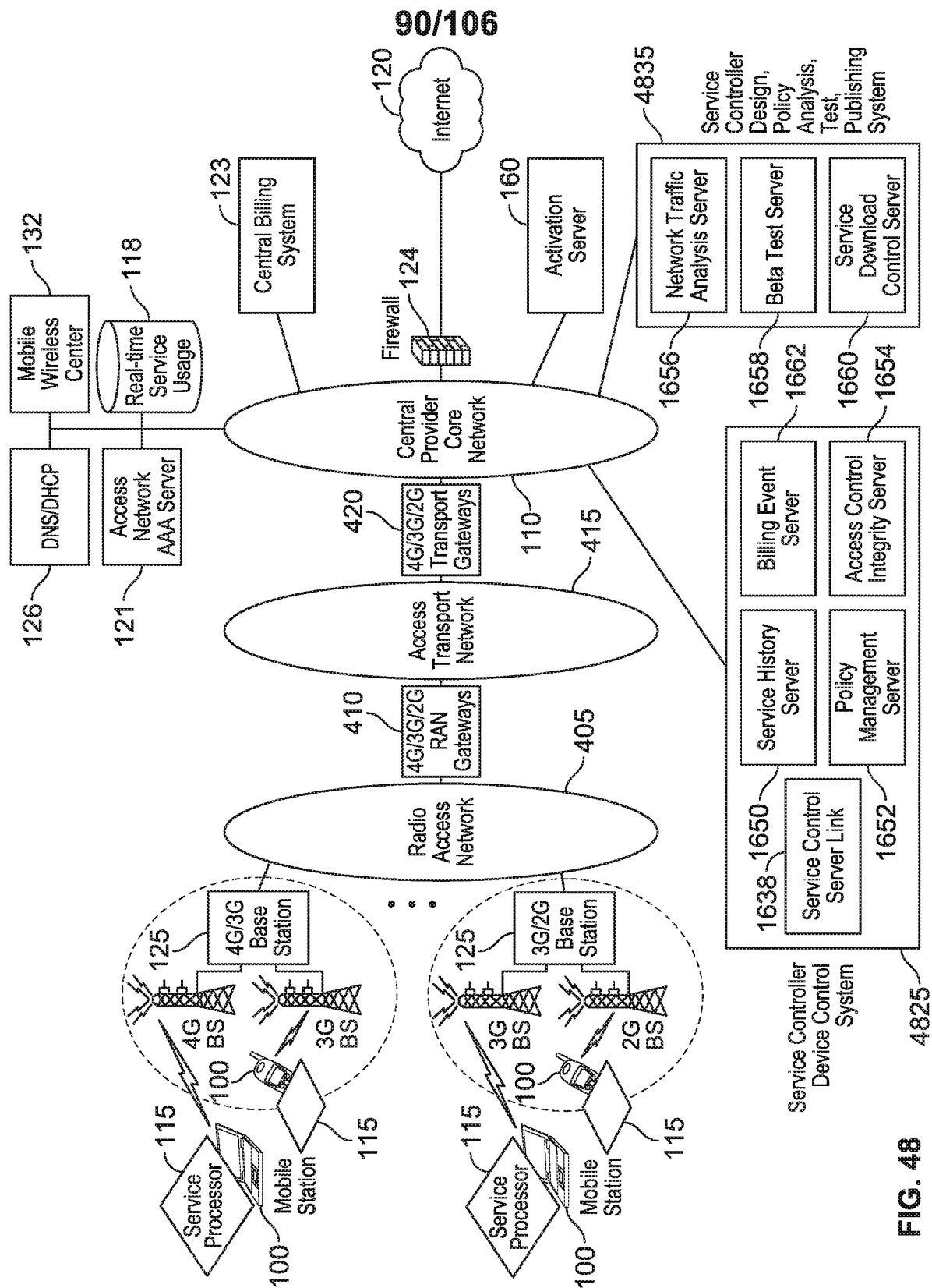


FIG. 48

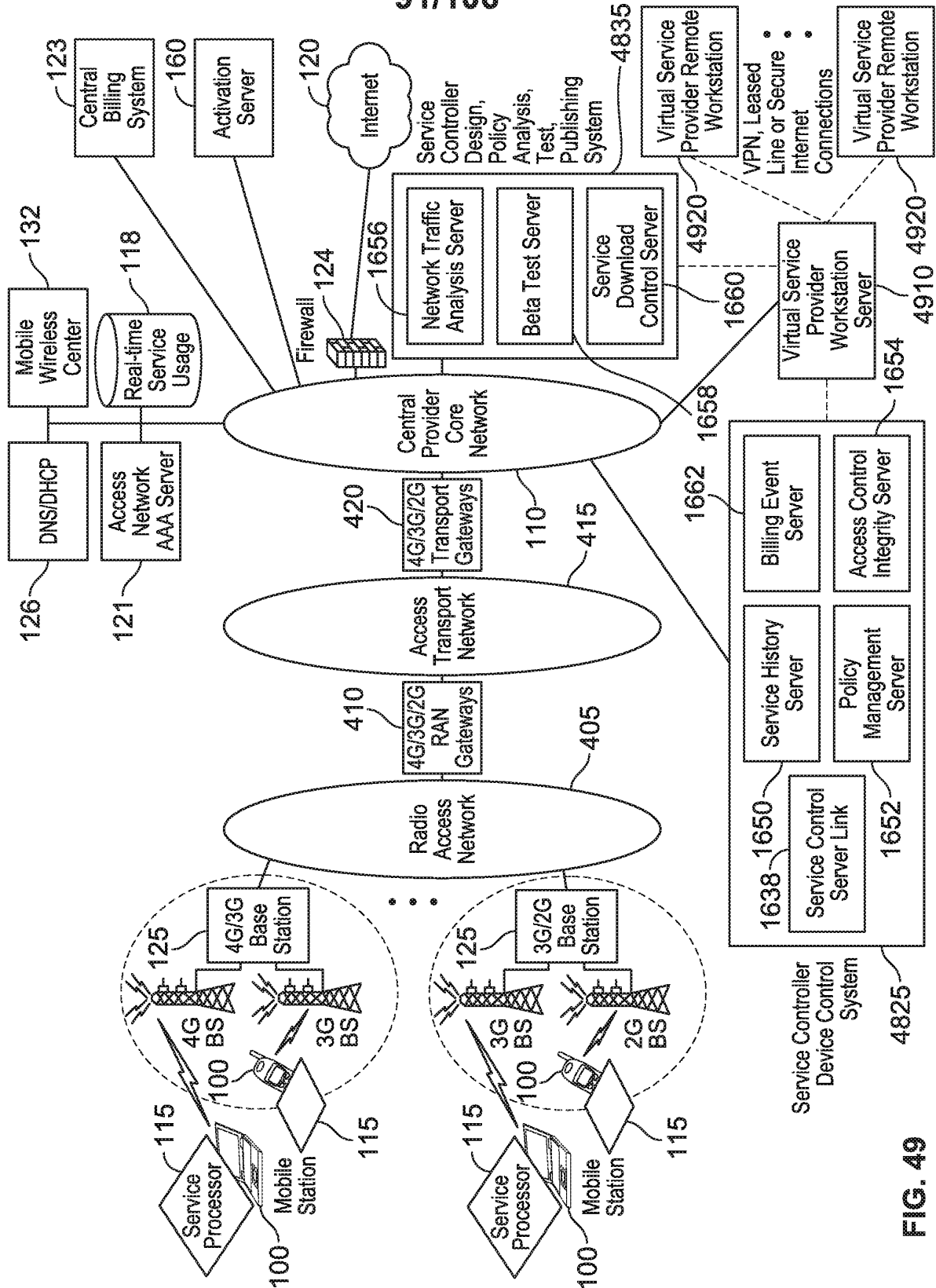


FIG. 49

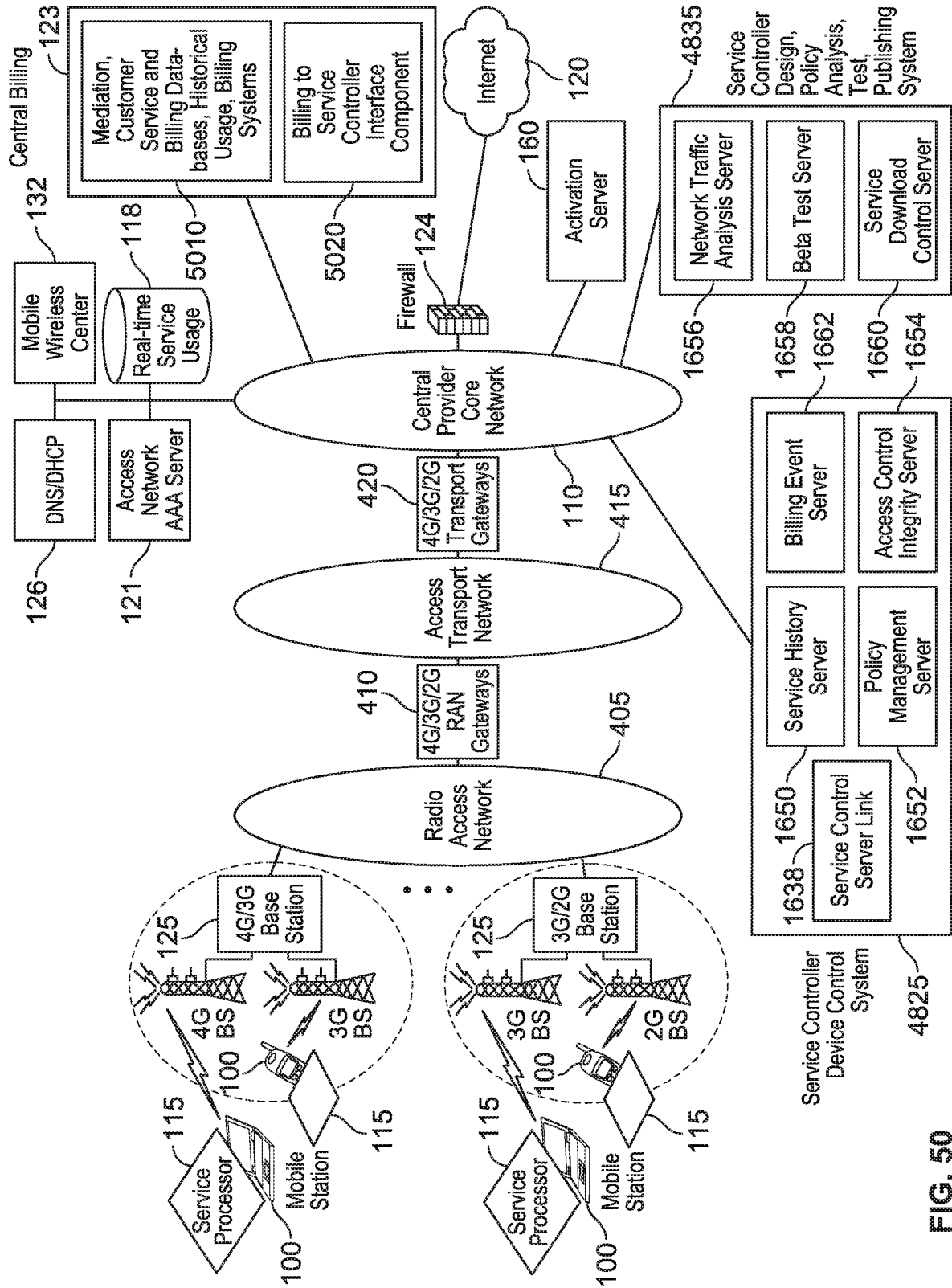


FIG. 50

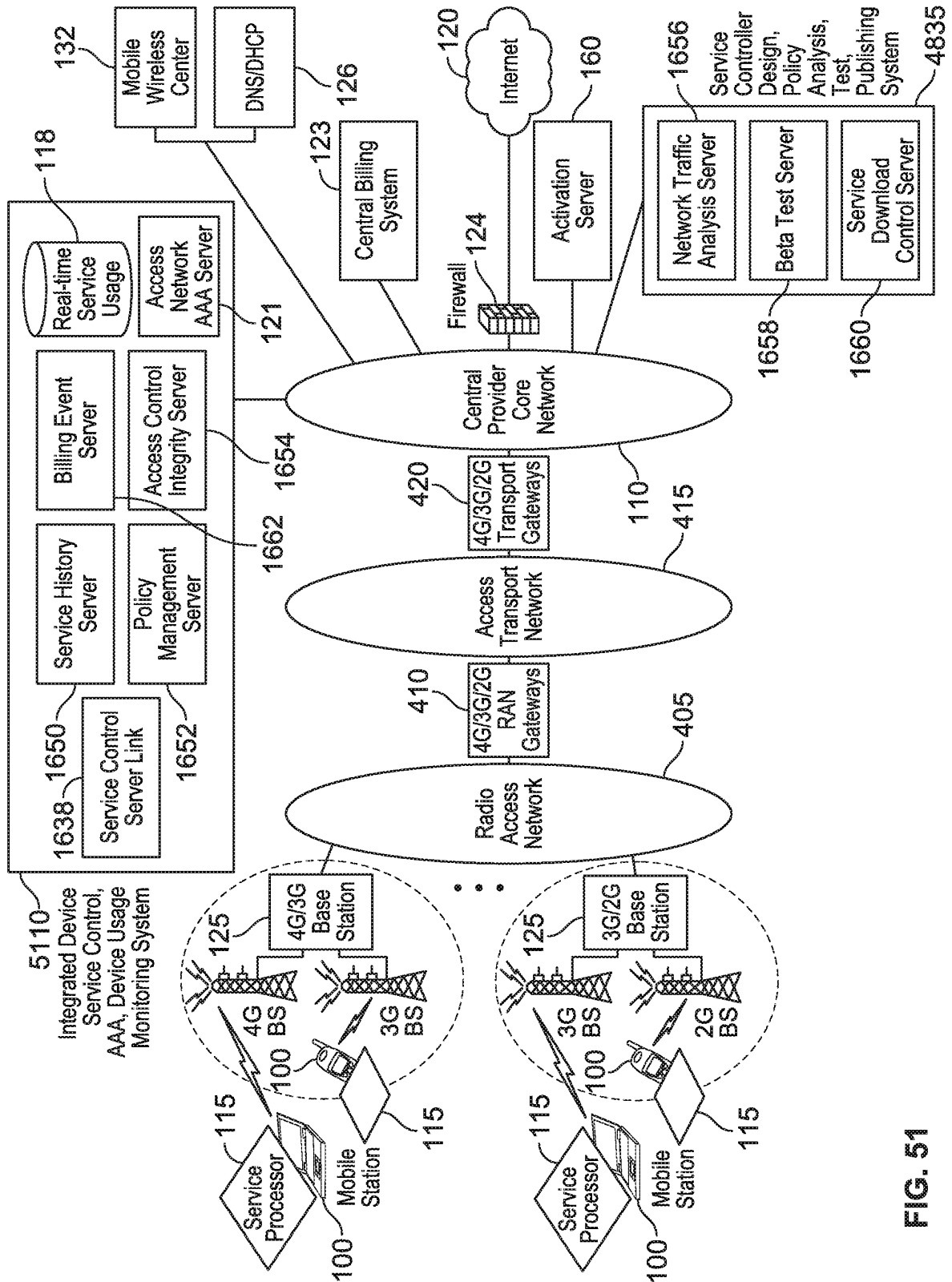


FIG. 51

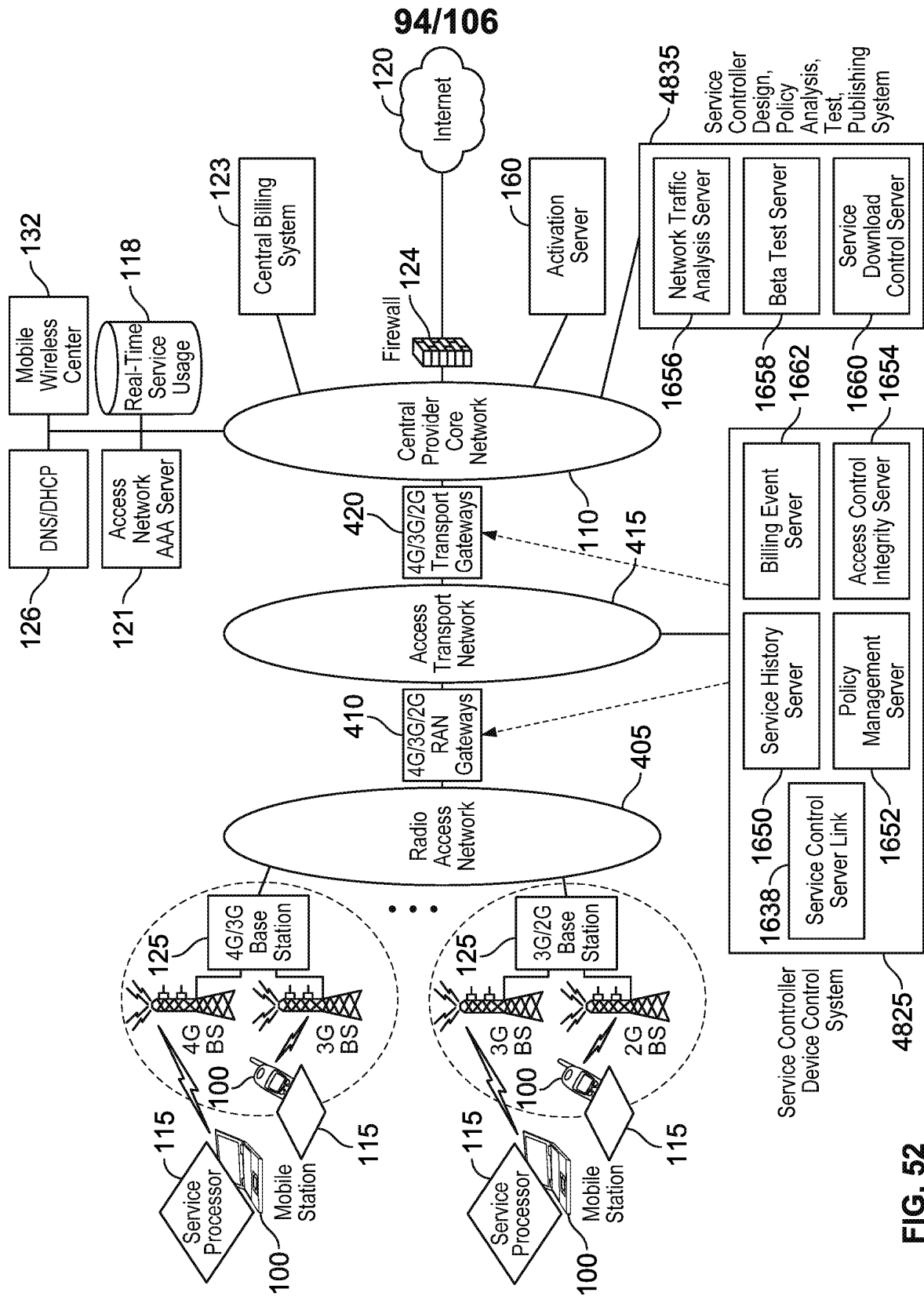


FIG. 52

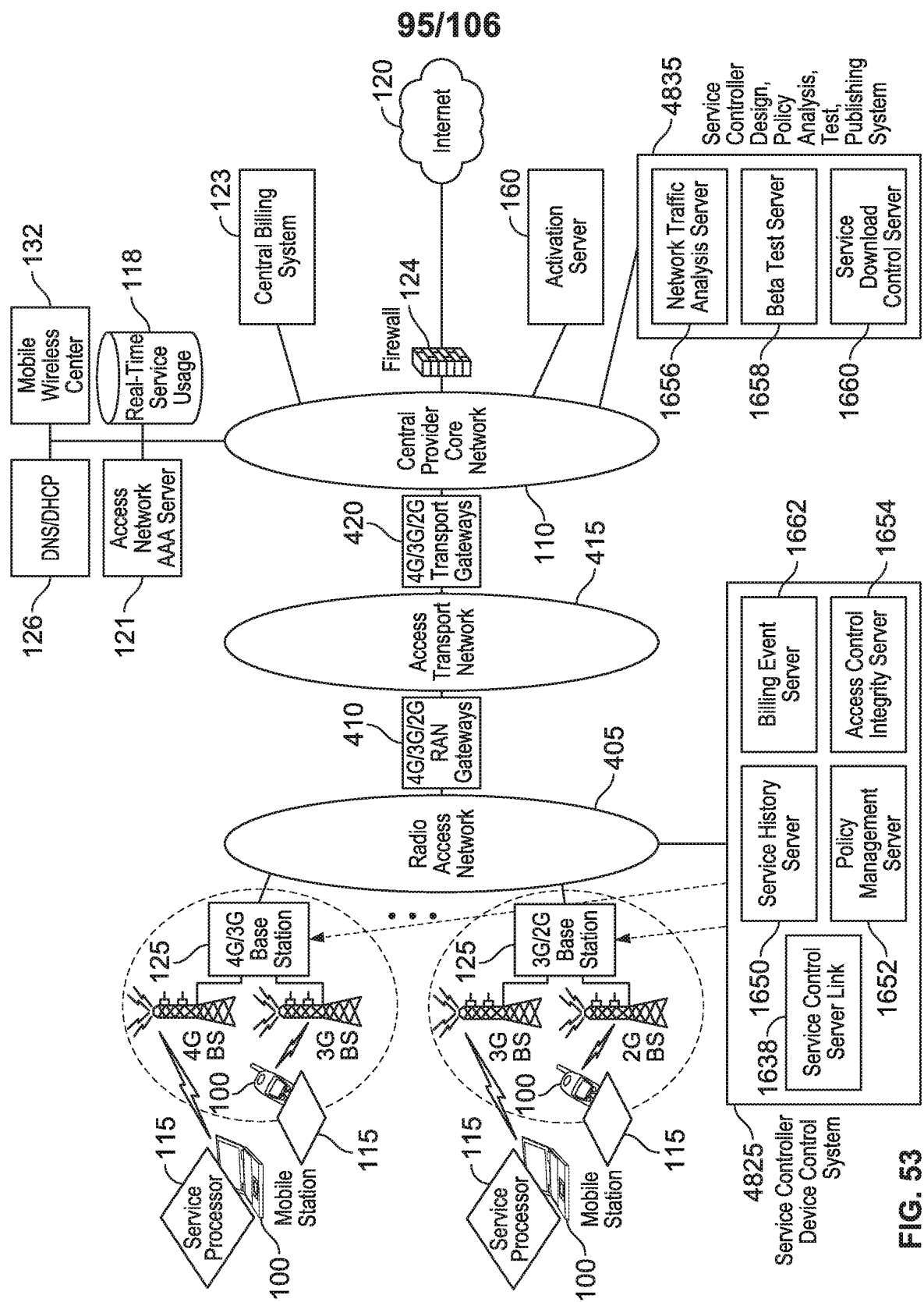


FIG. 53

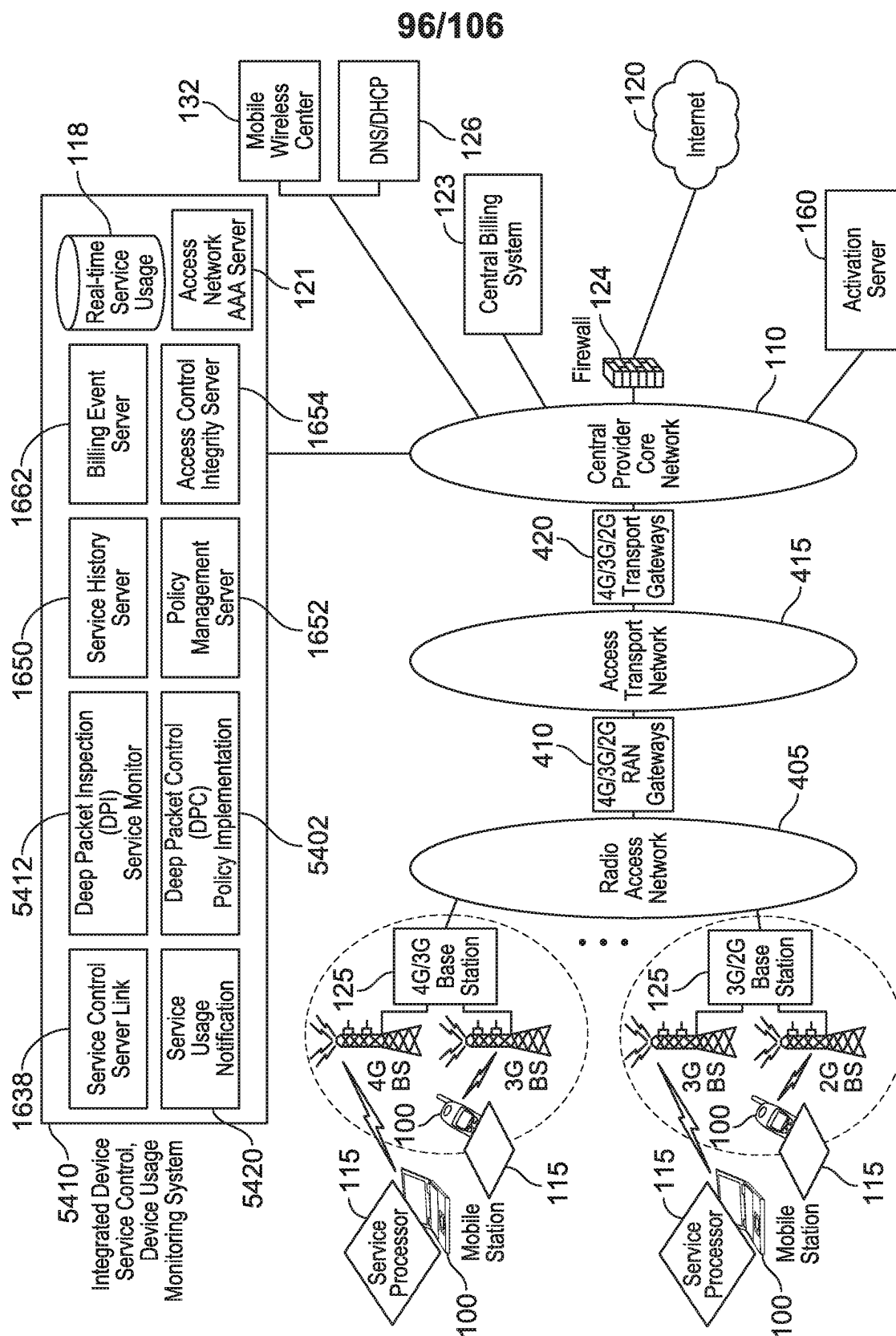


FIG. 54

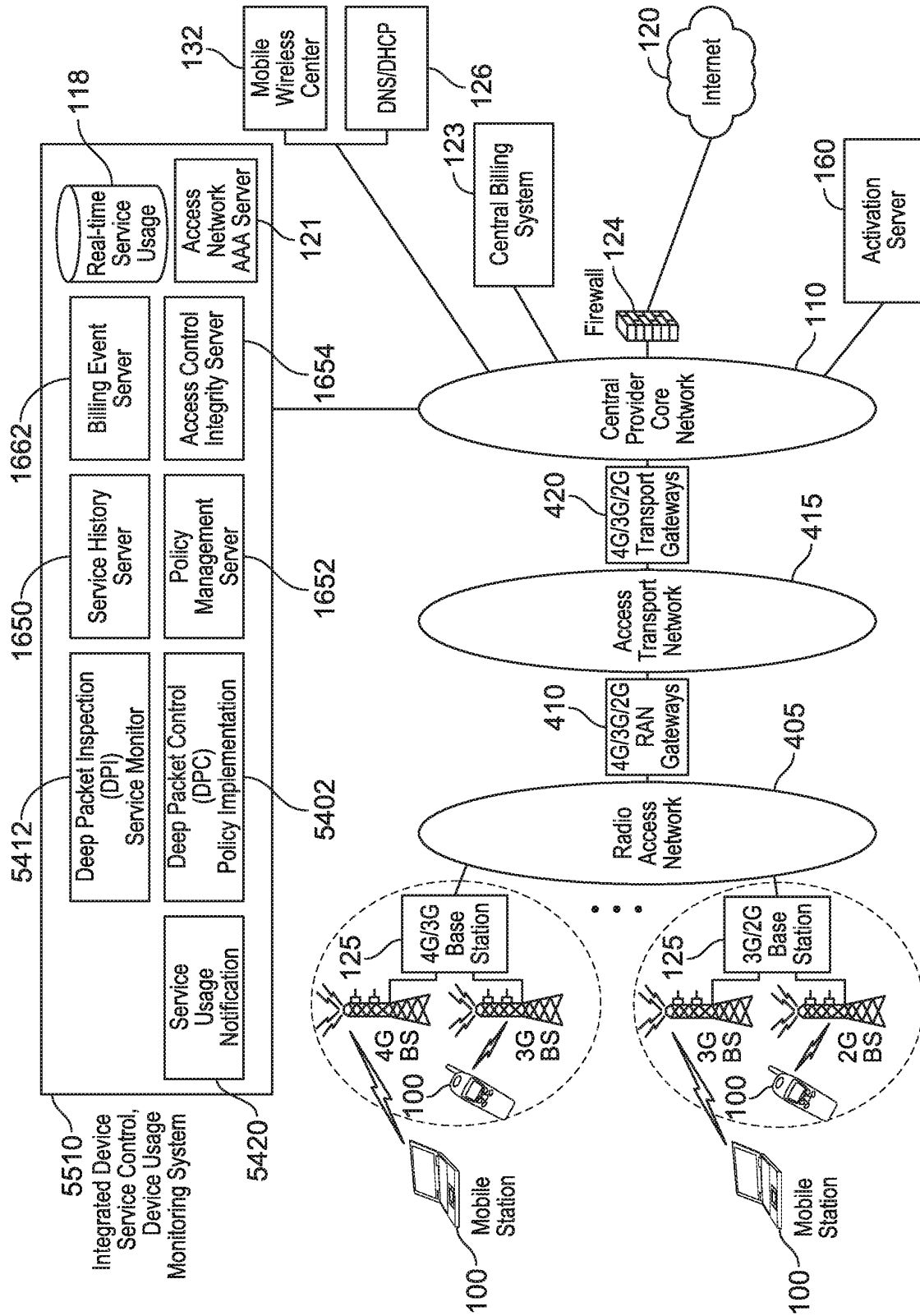


FIG. 55

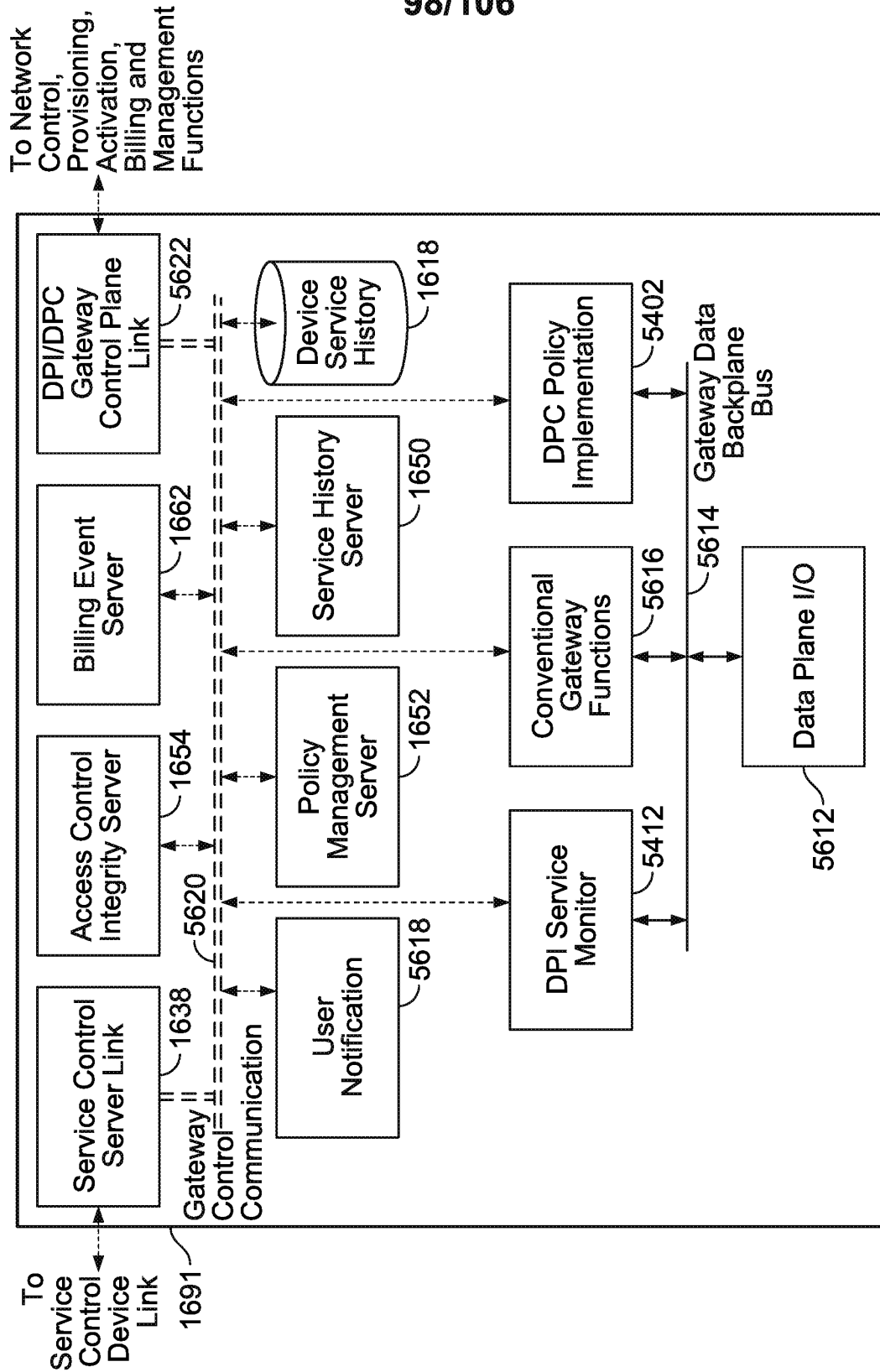


FIG. 56

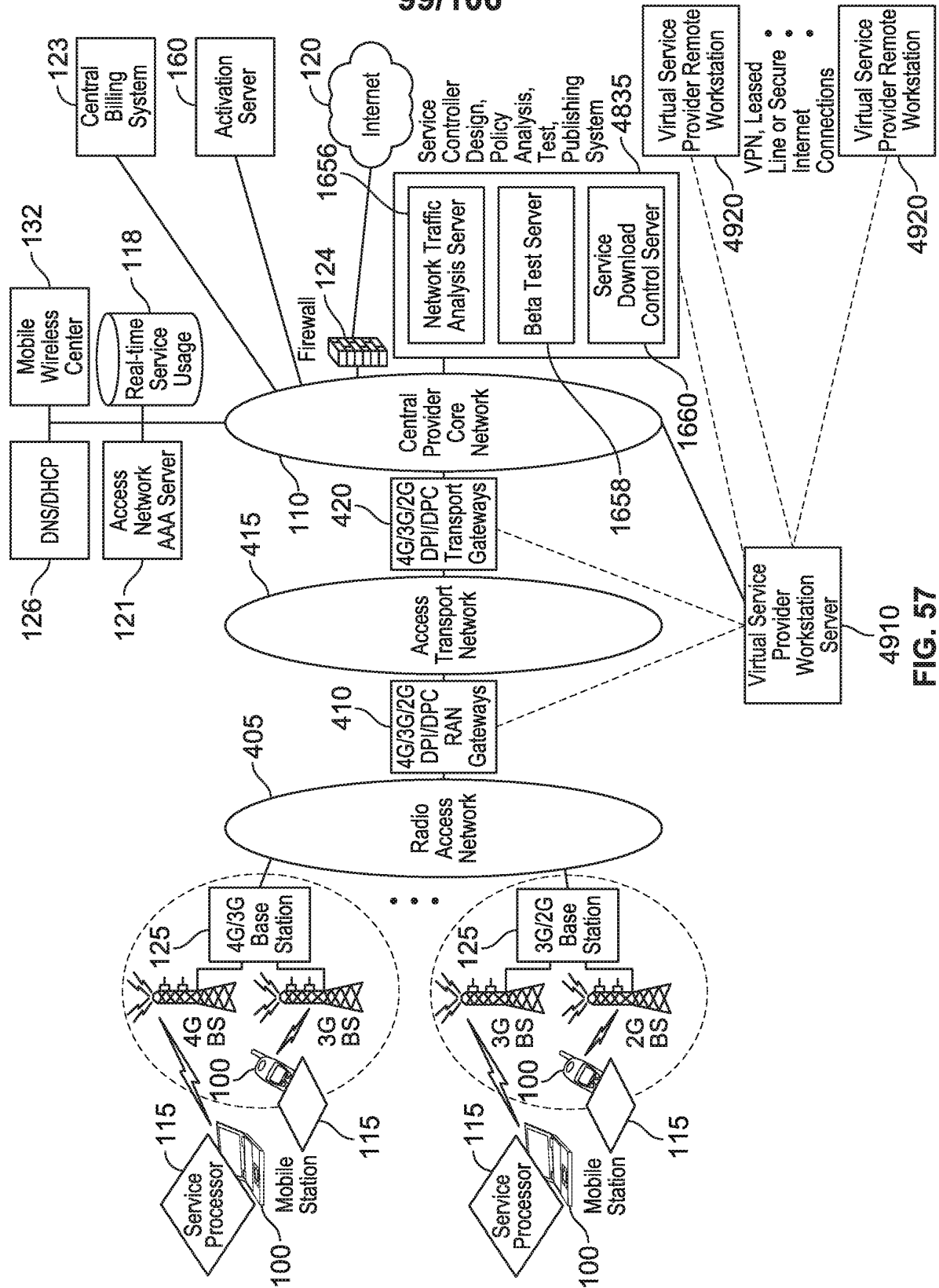


FIG. 57

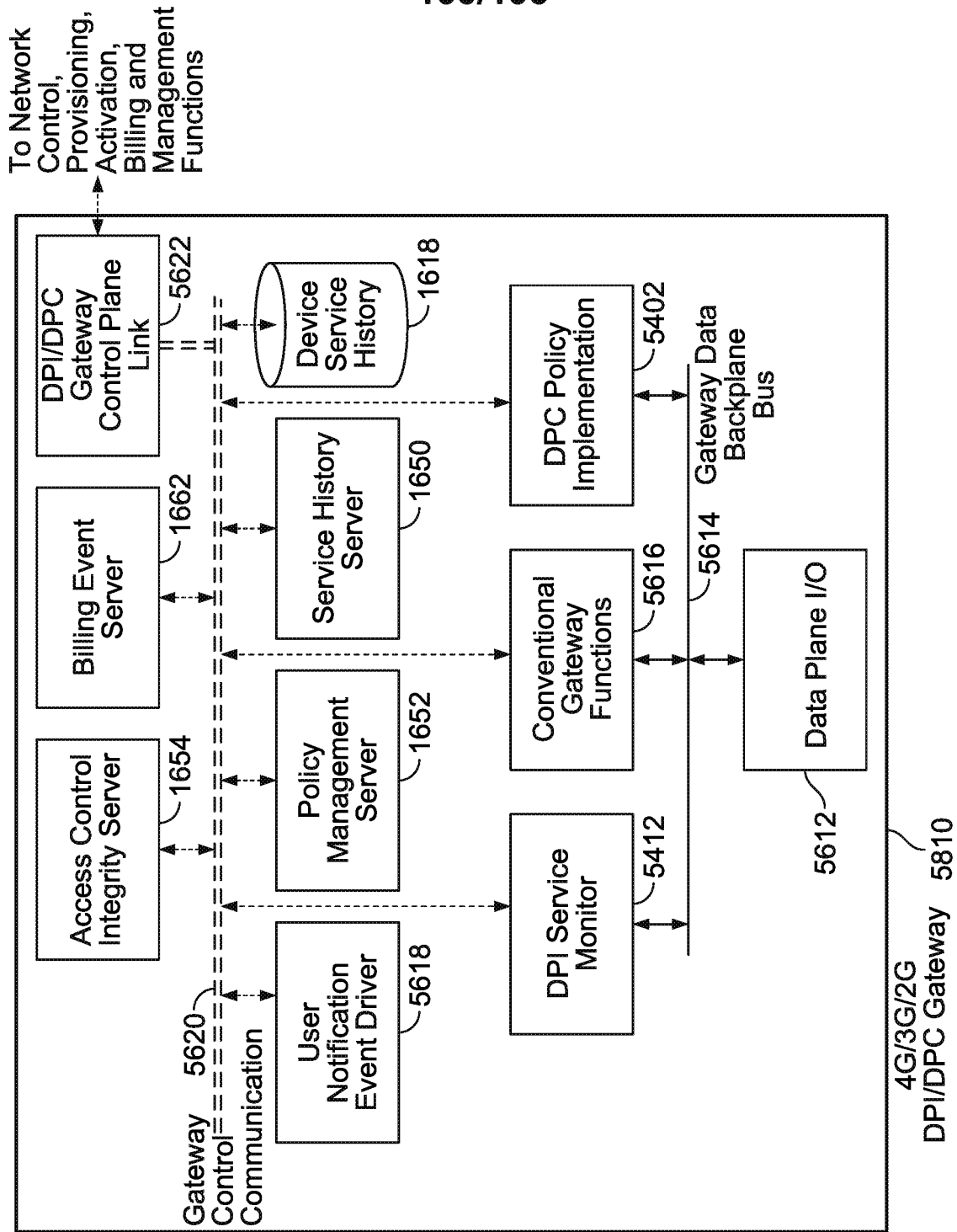


FIG. 58

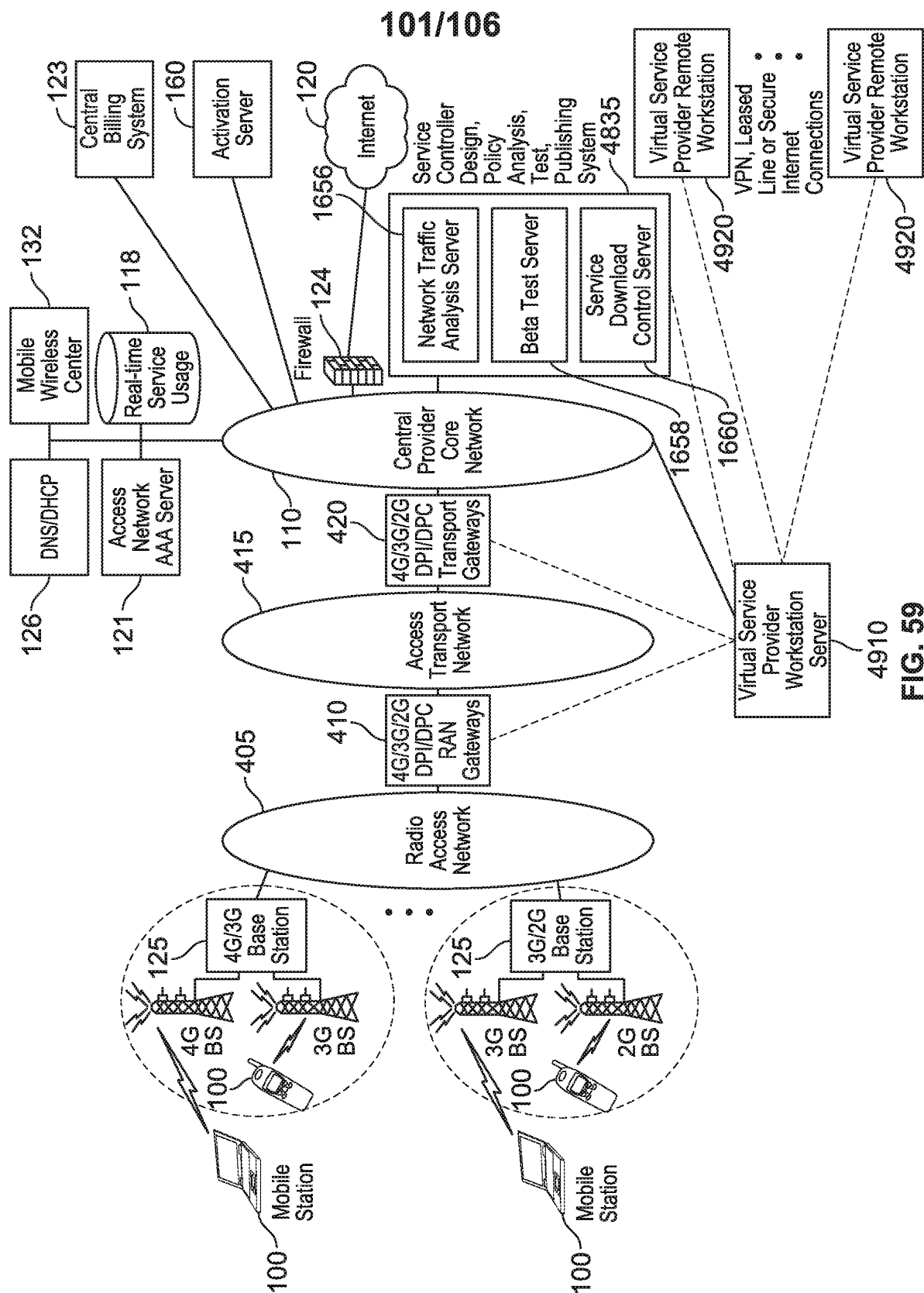
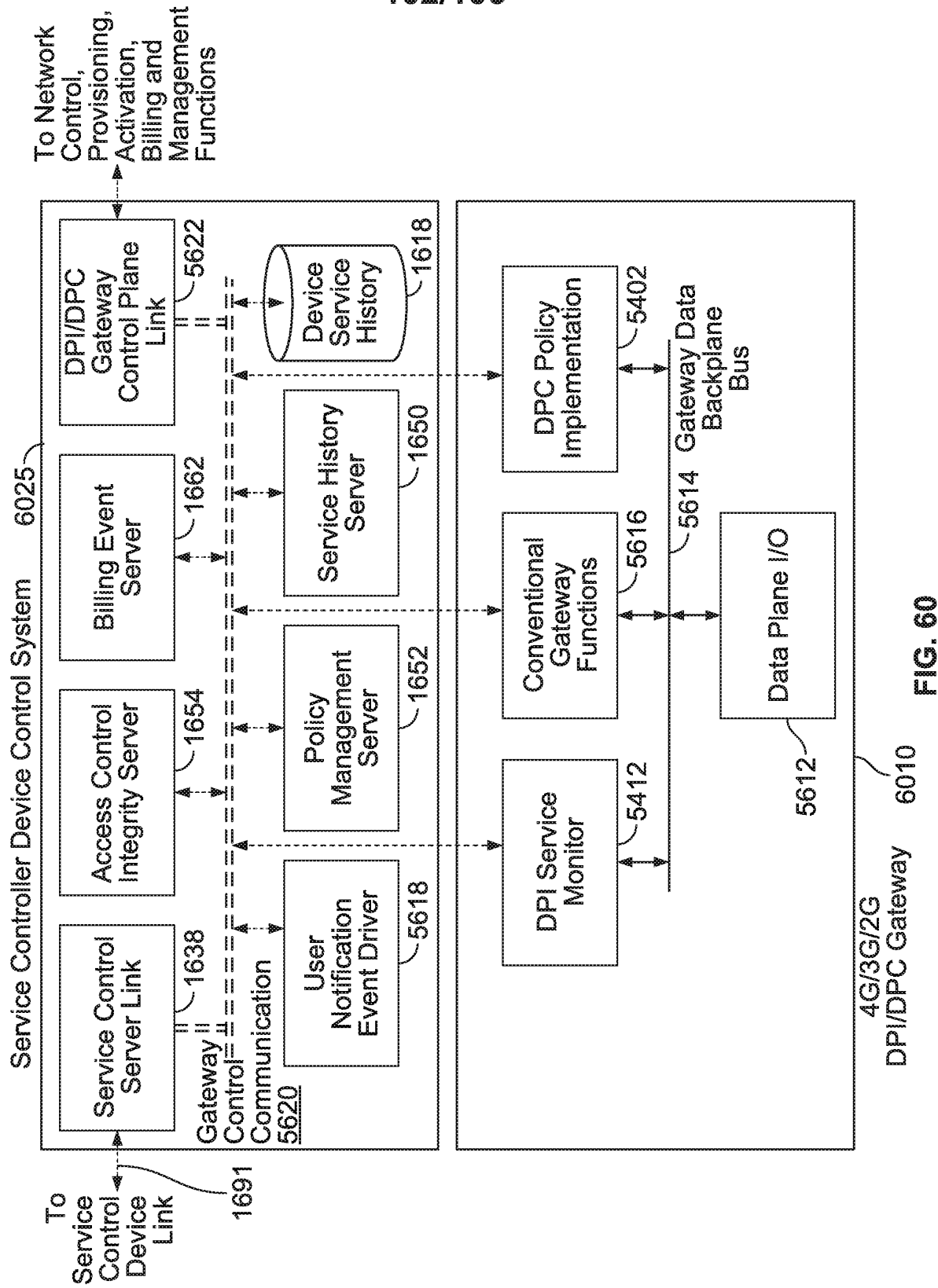


FIG. 59

101/106



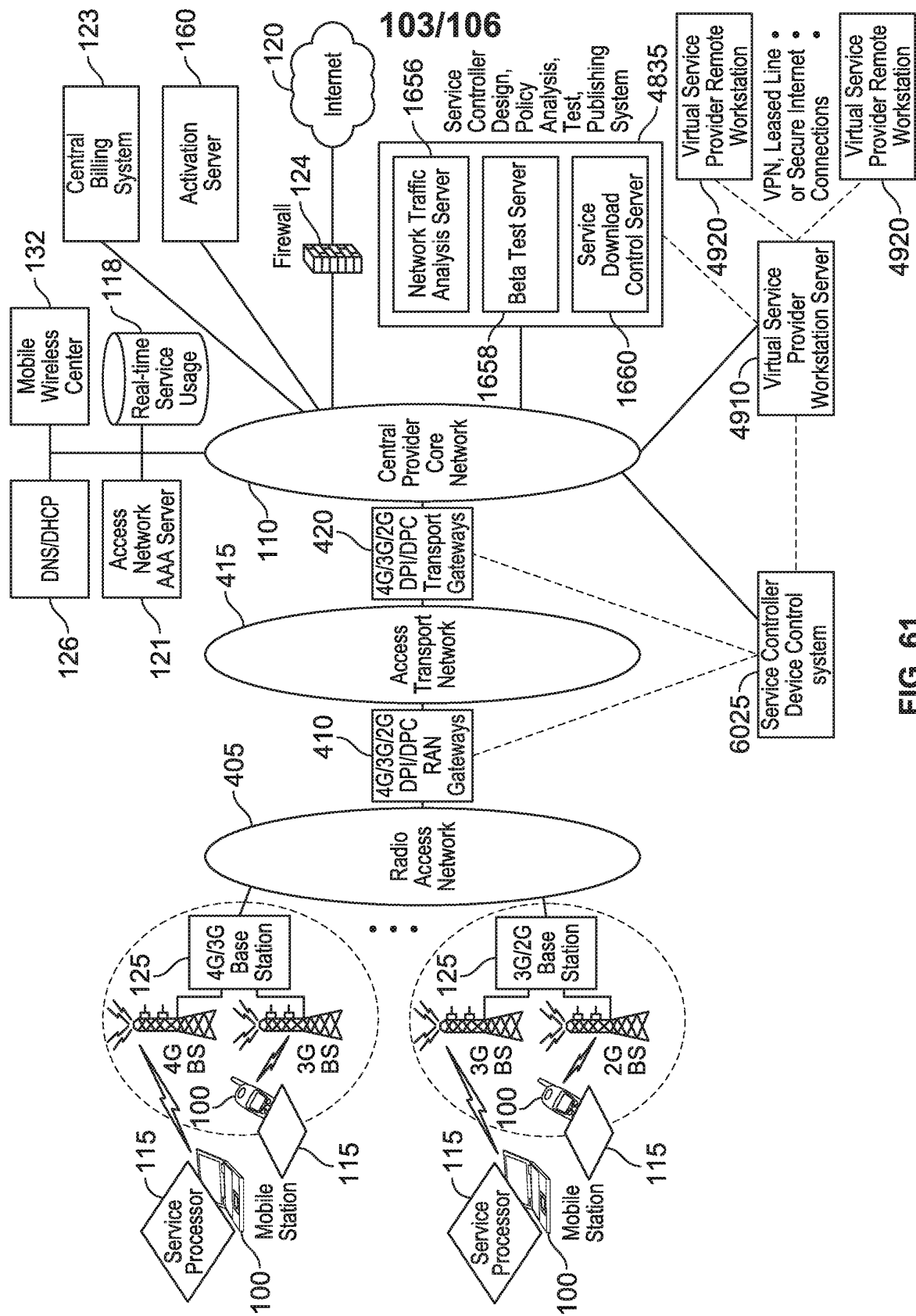


FIG. 61

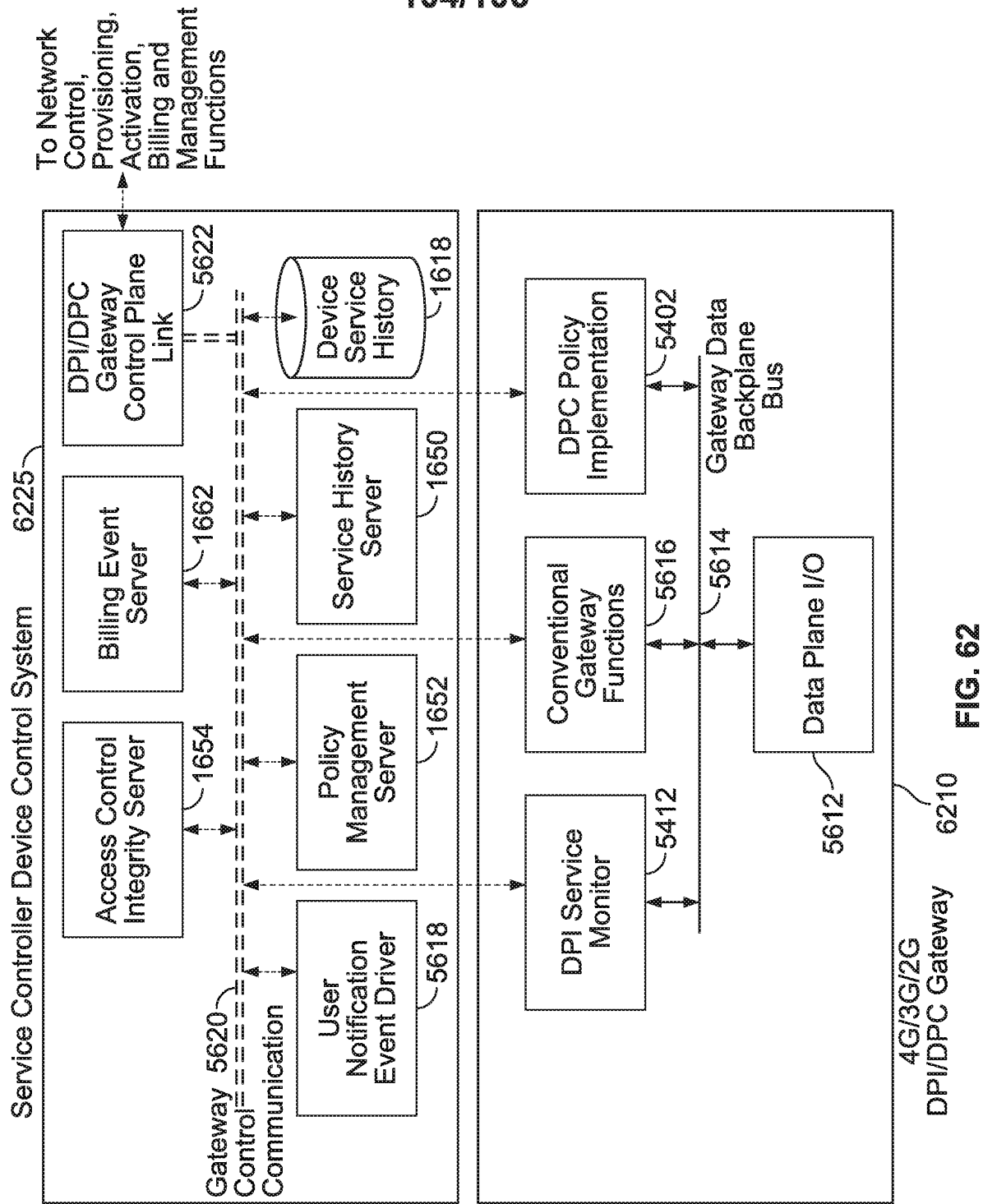


FIG. 62

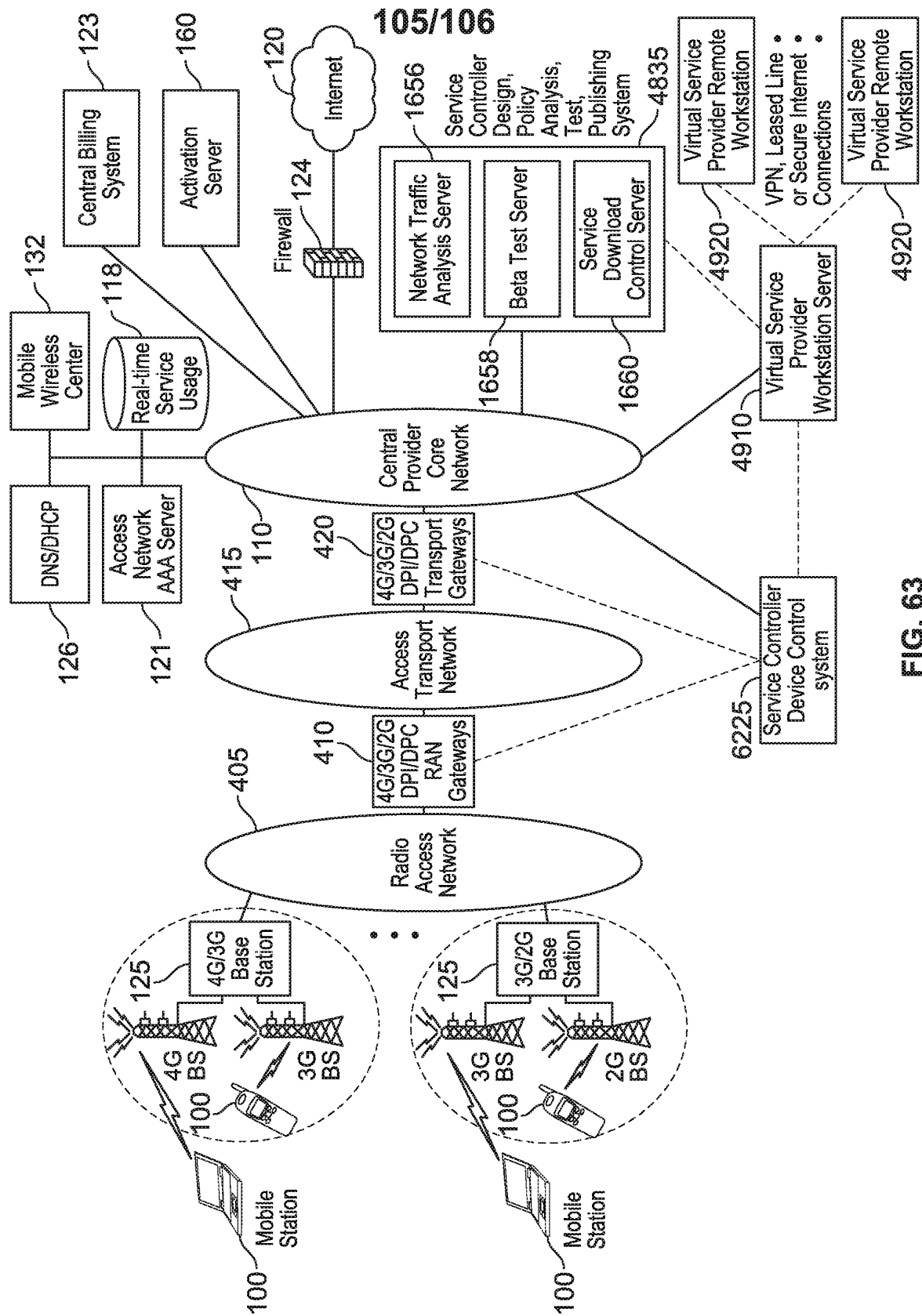


FIG. 63

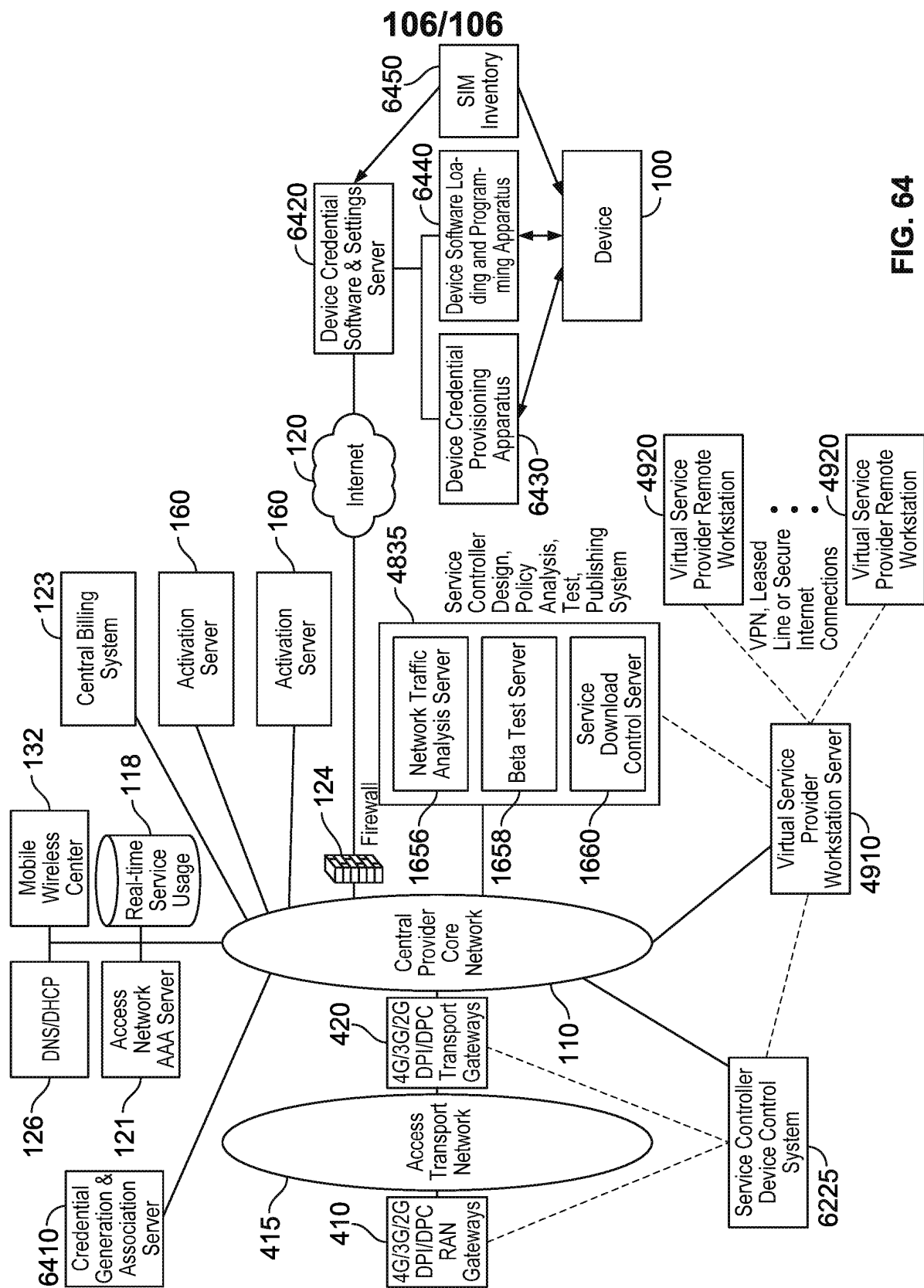


FIG. 64

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2:

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor	1				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Gregory	G.	Raleigh			
Residence Information (Select One) • US Residency Non US Residency Active US Military Service						
City	Incline Village	State/Province	NV	Country of Residence	US	
Mailing Address of Inventor:						
Address 1	110 N. College Avenue					
Address 2	Suite 1116					
City	Tyler	State/Province	TX			
Postal Code	75702	Country	US			
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.						
Add						

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.			
For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence information of this application.			
Customer Number	106963		
Email Address	patent@headwaterllc.com	Add Email	Remove Email

Application Information:

Title of the Invention	Automated Device Provisioning and Activation		
Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	106	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	106963		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
this application	Continuation of	16436628	2019-06-10

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		RALEP007C11C3C2C3C2C1C1C1	
		Application Number			
Title of Invention		Automated Device Provisioning and Activation			

Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16436628	Continuation of	15582350	2017-04-28	10321320	2019-06-11
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15582350	Continuation of	15239398	2016-08-17	9641957	2017-05-02
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
15239398	Continuation of	14979233	2015-12-22	9532161	2016-12-27
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14979233	Continuation of	14667353	2015-03-24	9232403	2016-01-05
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14667353	Continuation of	14263604	2014-04-28	9037127	2015-05-19
Prior Application Status		Patented		Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14263604	Continuation of	12380780	2009-03-02	8839388	2014-09-16
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61206354	2009-01-28		
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61206944	2009-02-04		
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61207393	2009-02-10		
Prior Application Status		Expired		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)		
12380780	Claims benefit of provisional	61207739	2009-02-13		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant	1	<input type="button" value="Remove"/>	
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>			
		<input type="button" value="Clear"/>	
☒ Assignee	Legal Representative under 35 U.S.C. 117		Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>			
Name of the Deceased or Legally Incapacitated Inventor: <div style="border: 1px solid black; width: 400px; height: 20px;"></div>			
If the Applicant is an Organization check here. ☒			
Organization Name	Headwater Research LLC		
Mailing Address Information For Applicant:			
Address 1	110 N. College Avenue		
Address 2	Suite 1116		
City	Tyler	State/Province	TX
Country	US	Postal Code	75702
Phone Number	903-201-6212	Fax Number	
Email Address	patent@headwaterllc.com		
Additional Applicant Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

Assignee 1			
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
			<input type="button" value="Remove"/>
If the Assignee or Non-Applicant Assignee is an Organization check here. ☒			
Organization Name	Headwater Research LLC		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	110 N. College Avenue		
Address 2	Suite 1116		
City	Tyler	State/Province	TX
Country i	US	Postal Code	75702
Phone Number	903-201-6212	Fax Number	
Email Address	patent@headwaterllc.com		
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet must be signed by a patent practitioner if one or more of the applicants is a juristic entity (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, all joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of all joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/James E. Harris/		Date (YYYY-MM-DD)	2022-01-17	
First Name	James E.	Last Name	Harris	Registration Number	40013
Additional Signature may be generated within this form by selecting the Add button.				<input type="button" value="Add"/>	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP007C11C3C2C3C2C1C1C1
		Application Number	
Title of Invention	Automated Device Provisioning and Activation		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

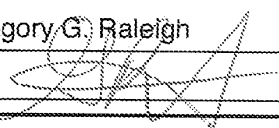
Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	AUTOMATED DEVICE PROVISIONING AND ACTIVATION
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: ☒ The attached application, or ☐ United States application or PCT international application number _____ filed on _____</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p> <p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Gregory G. Raleigh</u> Date (Optional) : _____</p> <p>Signature: <u></u></p> <p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	44760065
Application Number:	17577237
International Application Number:	
Confirmation Number:	5850
Title of Invention:	Automated Device Provisioning and Activation
First Named Inventor/Applicant Name:	GREGORY RALEIGH
Customer Number:	106963
Filer:	James E. Harris/Jennifer Smith
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP007C11C3C2C3C2C1C1C1
Receipt Date:	17-JAN-2022
Filing Date:	
Time Stamp:	16:26:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Specification	final_spec.pdf	1088044	no	240
			b20c005fc37dc26a85cb08a06984c410d0cf4f50		

Warnings:

Information:					
2	Claims	CLAIMS.pdf	37070	no	1
			0da64783b669704fb29131c2bcd8b930605ccc6		
Warnings:					
Information:					
3	Abstract	abstract.pdf	38019	no	1
			400aab7ff5af812024b45f62fa42be5c00bfff62c		
Warnings:					
Information:					
4	Drawings-only black and white line drawings	Drawings.pdf	10157110	no	106
			a620d6d5a3712df05a679648f6b3c9d78a6d2c29		
Warnings:					
Information:					
5	Application Data Sheet	ADS.pdf	1823813	no	9
			cac0177f8f73de1d591555ea702eb78ed0c54ef3		
Warnings:					
Information:					
6	Oath or Declaration filed	Raleigh_Declaration.pdf	99297	no	1
			f767b71a3d35b8e258cd5b2b75cb8e48ce66a9b		
Warnings:					
Information:					
Total Files Size (in bytes):			13243353		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.