PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.
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.

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	State/Province	Country of Residence
Woodside	CA	US

Mailing Address of Inventor:

Address 1	1011 Pruitt Place
Address 2	
City	Tyler
State/Province	TX
Postal Code	75703
Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jeffrey		Green	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	State/Province	Country of Residence
Sunnyvale	CA	US

Mailing Address of Inventor:

Address 1	1011 Pruitt Place
Address 2	
City	Tyler
State/Province	TX
Postal Code	75703
Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	James		Lavine	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

City	Corte Madera	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	**State/Province**	TX
Postal Code	75703	**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	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems		
Attorney Docket Number	RALEP041D1C1	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	47	**Suggested Figure for Publication (if any)**	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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)
thisapplication	Continuation of	14340270	2014-07-24
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14340270	Division of	13309463	2011-12-01	8793758	2014-07-29

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61418507	2010-12-01
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61418509	2010-12-01
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61420727	2010-12-07

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61422565	2010-12-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61422572	2010-12-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61422574	2010-12-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61435564	2011-01-24
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61472606	2011-04-06
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61550906	2011-10-24
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13309463	Continuation in part of	13237827	2011-09-20	8832777	2014-09-09
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13309463	Continuation in part of	13134028	2011-05-25	8589541	2013-11-19
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13309463	Continuation in part of	13253013	2011-10-04	8745191	2014-06-03

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13237827	Claims benefit of provisional	61384456	2010-09-20
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13237827	Continuation in part of	12695019	2010-01-27	8275830	2012-09-25

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695019	Claims benefit of provisional	61270353	2009-07-06
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695019	Claims benefit of provisional	61264126	2009-11-24
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61348022	2010-05-25
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61381159	2010-09-09
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61381162	2010-09-09
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61385020	2010-09-21
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61387243	2010-09-28

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61387247	2010-09-28
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61407358	2010-10-27
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12694455	2010-01-27	8402111	2013-03-19

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	13134005	2011-05-25	8635335	2014-01-21

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12695021	2010-01-27	8346225	2013-01-01

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12694455	Claims benefit of provisional	61264120	2009-11-24
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695021	Claims benefit of provisional	61252153	2009-10-15
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12695021	Continuation in part of	12380780	2009-03-02	8839388	2014-09-16

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134005	Continuation in part of	12380778	2009-03-02	8321526	2012-11-27

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134005	Continuation in part of	12380780	2009-03-02	8839388	2014-09-16

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13253013	Claims benefit of provisional	61389547	2010-10-04
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13253013	Continuation in part of	12695020	2010-01-27	8406748	2013-03-26

Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13253013	Continuation in part of	12694445	2010-01-27	8391834	2013-03-05

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695020	Claims benefit of provisional	61275208	2009-08-25
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695020	Claims benefit of provisional	61237753	2009-08-28
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12694445	Claims benefit of provisional	61252151	2009-10-15
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380778	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)
12380778	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)
12380778	Claims benefit of provisional	61207393	2009-02-10

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380778	Claims benefit of provisional	61207739	2009-02-13
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
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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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 — Remove

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.

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:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Headwater Partners I LLC		
Mailing Address Information For Applicant:			
Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	**State/Province**	TX
Country	US	Postal Code	75703
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. 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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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)	2016-10-06
First Name	James E.	Last Name	Harris	Registration Number	40013

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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 CooperationTreaty.

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.

BACKGROUND

[0001] As the computing power of mobile end-user devices has increased, mobile devices have become capable of sending and receiving increasing amounts of data. In addition to e-mail and text messages, many of today's mobile devices can support a variety of applications that send large quantities of information to and from end users. For example, in addition to sending e-mail and text messages, many of today's mobile devices can deliver news, weather, sports, maps, social networking information, music, videos, high-resolution photographs, documents, presentations, and other kinds of information.

[0002] The ability of mobile devices to send and receive such a wide variety and large quantity of data has stressed wireless access network bandwidth capabilities. As a result, network operators are either eliminating service plans with unlimited data usage, or they are increasing the price of unlimited service plans so that such plans are not attractive to most consumers. Consequently, many users of mobile end-user devices subscribe to service plans that include only a limited amount of data per fixed time period (e.g., per month). Because today's mobile end-user devices can access (e.g., send or receive) large amounts of information, there is a potential for a user of a mobile device to exceed his or her data plan allowance without realizing it. It is well known that such "overages" in data usage can be very expensive because the billing rate for data usage exceeding the contracted service plan amount is often significantly higher than the billing rate under the service plan.

[0003] Because of their computing capabilities, many of today's mobile end-user devices can also participate in the implementation and enforcement of service policies associated with access network service plans, such as charging, control, and notification policies. Device-assisted services (DAS) have been described in the many prior applications listed in the "Cross Reference to Related Applications" section of this document. When end-user devices participate in implementing and enforcing access network policies, there is a potential for device users to attempt to, or to successfully, spoof or hack end-user device components to fraudulently obtain access to data services at incorrect, lower service usage billing rates. Likewise, highly motivated users might try

IPR2025-01572
Apple EX1002 Page 15

to gain access to network elements that perform functions related to service policy implementation or enforcement associated with the end-user device's data usage.

[0004] Thus, there is a need to secure software and hardware, in both end-user devices and in network elements, involved in the provision of device-assisted services. In addition, there is a need to detect and mitigate fraudulent or potentially fraudulent activities.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The present invention, in accordance with one or more various embodiments, is described in detail with reference to the following figures. The drawings are provided for purposes of illustration only and merely depict typical or example embodiments of the invention. These drawings are provided to facilitate the reader's understanding of the invention and shall not be considered limiting of the breadth, scope, or applicability of the invention. It should be noted that for clarity and ease of illustration these drawings are not necessarily made to scale.

[0006] Figure 1 illustrates the various components of a device-assisted services (DAS) implementation in accordance with some embodiments.

[0007] Figure 2 illustrates an example embodiment of a device-based service processor system in communication with a network-based service controller system.

[0008] Figure 3 illustrates an example embodiment of functional elements for a network access service policy implementation.

[0009] Figure 4 illustrates an example embodiment of a secure service controller architecture for DAS systems.

[0010] Figure 5 illustrates an example embodiment of a secure service controller architecture for DAS systems.

[0011] Figure 6 illustrates an example embodiment of a secure service controller architecture for DAS systems.

IPR2025-01572
Apple EX1002 Page 16

[0012] Figure 7 illustrates communications within an applications security zone in accordance with some embodiments.

[0013] Figure 8 illustrates an example embodiment that provides geo-redundancy.

[0014] Figure 9 illustrates an example embodiment of a service controller portal function.

[0015] Figure 10 illustrates an example embodiment of a service controller file transfer function.

[0016] Figure 11 illustrates an example embodiment of a service controller gateway function.

[0017] Figure 12 illustrates an example embodiment of a service controller credentialing function.

[0018] Figure 13 illustrates an example embodiment of a service controller EAI server that supports various communication paths.

[0019] Figure 14 illustrates an example embodiment of a service controller EAI server that supports various communication paths.

[0020] Figure 15 illustrates an example embodiment of a service controller EAI server that supports various communication paths.

[0021] Figure 16 illustrates an example embodiment of a service controller EAI server that supports various communication paths.

[0022] Figure 17 illustrates an example embodiment of a service controller fraud server.

[0023] Figure 18 illustrates an example embodiment of a service controller reconciliation server.

[0024] Figure 19 illustrates an example embodiment of a service controller

IPR2025-01572
Apple EX1002 Page 17

message bus.

[0025] Figure 20 illustrates an example embodiment that includes two data centers.

[0026] Figure 21 illustrates a set of steps an end-user device performs to obtain a credential with a service controller in accordance with some embodiments.

[0027] Figure 22 illustrates a set of steps a service controller performs to provide a credential to a service processor in accordance with some embodiments.

[0028] Figure 23 illustrates an procedure a service controller performs to allocate credentials to multiple end-user devices in accordance with some embodiments.

[0029] Figure 24 illustrates an example embodiment of a process to start or stop a data session with SGSN notification.

[0030] Figure 25 illustrates an example embodiment of a process to start or stop a data session with GGSN notification.

[0031] Figure 26 illustrates an example embodiment of a process to start or stop a data session when a AAA or RADIUS server provides start/stop accounting in a GSM/GPRS core data network.

[0032] Figure 27 illustrates an example embodiment of a process to start or stop a data session when an OCS provides start/stop accounting in a GSM/GPRS core data network.

[0033] Figure 28 illustrates an example embodiment of a procedure that a verifying software component on an end-user device may perform to verify the integrity of another software component on the end-user device.

[0034] Figure 29 illustrates an example embodiment of a procedure that a to-be-verified software component can perform in response to the procedure illustrated in Figure 28.

IPR2025-01572
Apple EX1002 Page 18

[0035] Figure 30 illustrates an example embodiment of a procedure to determine whether to allow a modification, update, or replacement of an software program installed on an end-user device.

[0036] Figure 31 illustrates an example embodiment of a procedure that an end-user device can use to validate that an application installed on the end-user device is authentic.

[0037] Figure 32 illustrates an example embodiment of a procedure that a service controller can use to validate that an application installed on an end-user device is authentic.

[0038] Figure 33 illustrates an example embodiment of a procedure that a service controller can use to validate that an application installed on an end-user device is authentic.

[0039] Figure 34 illustrates an example embodiment of a procedure that an end-user device can use to validate that an application installed on the end-user device is authentic.

[0040] Figure 35 illustrates an example embodiment of a procedure that a service controller can use to validate that an application installed on an end-user device is authentic.

[0041] Figure 36 illustrates an example embodiment of a procedure that an end-user device can use to validate that an application installed on the end-user device is authentic.

[0042] Figure 37 illustrates an example embodiment of a procedure that a service controller can use to validate that an application installed on an end-user device is authentic.

[0043] Figure 38 illustrates an example embodiment of an end-user device for implementing access network policy specific to a device application program.

IPR2025-01572
Apple EX1002 Page 19

[0044] Figure 39 illustrates an example embodiment wherein an end-user device is capable of connecting to the Internet through more than one access network.

[0045] Figure 40 illustrates an example embodiment of a procedure that a service controller may use to verify a software component on an end-user device based on a verification message from the end-user device.

[0046] Figure 41 illustrates an example embodiment of a layered approach that a service controller can use to assess the likelihood that an end-user device is behaving fraudulently.

[0047] Figure 42 illustrates a layered approach to fraud detection in accordance with some embodiments.

[0048] Figure 43 illustrates an example embodiment of a service controller reconciliation processing procedure that may be used to detect fraud using information from and end-user device and information from a second source.

[0049] Figure 44 illustrates an example embodiment with network system elements that can be included in a service controller system to facilitate a DAS implementation and the flow of information between those elements.

[0050] Figure 45 illustrates an example embodiment of a procedure to detect when a user of an end-user device attempts to alter the end-user device's use of a time-based service plan by modifying the time setting on end-user device.

[0051] Figure 46 illustrates an example embodiment of a procedure to detect when a user of an end-user device attempts to alter the end-user device's use of a time-based service plan by modifying the time zone setting on end-user device.

[0052] Figure 47 illustrates a fraud detection approach in accordance with some embodiments.

[0053] Figure 48 illustrates an example embodiment of a procedure that a rule-based detection element may use to apply rules to detect fraud.

[0054] Figure 49 illustrates an example embodiment of a procedure that a static analysis element may use to determine fraud based on a statistical model.

[0055] Figure 50 illustrates an example embodiment of a procedure that a time-series analysis element may use to determine fraud based on a time-series model.

[0056] Figure 51 illustrates an example embodiment of a fraud-detection system that supports rule-based fraud detection and the application of statistical or time-series models in accordance with some embodiments.

SUMMARY

[0057] According to various embodiments, systems and methods are provided for securing device-assisted services (DAS) systems and for detecting and mitigating fraud in such systems.

[0058] In some embodiments, an end-user device comprises one or more modems to allow communications over a wireless access network, memory configured to store an application-specific network access policy to be applied when a particular application program attempts to communicate or successfully communicates over the wireless access network, and one or more device agents configured to detect attempted or successful activity by the particular application program and to apply the application-specific network access policy to the communication activity.

[0059] In some embodiments, the one or more device agents are configured to detect attempted or successful activity by the particular application program by flow-tagging a data flow associated with the particular application program, associating the flow tag with the application identifier, and applying the application-specific network access policy to the flow-tagged data flow.

[0060] In some embodiments, an end-user device comprises one or more modems to allow communications over a wireless access network, memory configured to store an application-specific network access policy to be applied when a particular application program attempts to communicate or successfully communicates over the wireless access

IPR2025-01572
Apple EX1002 Page 21

network, and one or more device agents configured to use an application programming interface (API) to arrange an application setting to assist in implementing the application-specific network access policy.

[0061] In some embodiments, the application-specific network access policy comprises a control policy configured to assist in controlling transmissions or receptions over the wireless access network that are associated with the application program. In some embodiments, the application-specific network access policy comprises a charging policy configured to assist in accounting for transmissions or receptions over the wireless access network that are associated with the application program. In some embodiments, the end-user device has a user interface, and the application-specific network access policy comprises a notification policy configured to assist in presenting, through the user interface, a notification message, such as, for example: an offer or an advertisement, information about a network type (e.g., a home network, a roaming network, a cellular network, a wireless wide-area network (WWAN), a wireless local area network (WLAN), a wireless personal area network (WPAN), a 2G network, a 3G network, a 4G network, a WiMAX network, an Ethernet network, a DSL network, a DOCSIS network, a cable network, a WiFi network, etc.), an indication of an amount or cost of data usage associated with the application program, an indication of a projected amount or a projected cost of data usage associated with the application program (e.g., a projection based on a past or historical data usage associated with the application program), an indication of an amount or cost of data usage associated with the application program during a particular period of time (possibly user-configured or user-selected), an indication that an amount or cost of data usage associated with the application satisfies a condition relative to a limit setting (e.g., exceeds a threshold, meets a threshold, is less than a threshold, etc.), an indication of an amount or cost of background data usage by the application program, etc. In some embodiments, the policy is associated with an application identifier (e.g., a credential associated with the application, possibly stored on the end-user device). In some embodiments, the application program is secured by an application credential (which may be the application identifier). In some embodiments, the one or more device agents are further configured to prevent modifications, updates, or replacements of the application program unless software purporting to be a modification,

IPR2025-01572
Apple EX1002 Page 22

update, or replacement of the application program is associated with a credential that is consistent with (e.g., matches) the application credential.

[0062] In some embodiments, at least one of the one or more device agents is secured by an agent credential, and one of the one or more device agents is configured to prevent modifications, updates, or replacements of the at least one of the one or more device agents unless software purporting to be a modification, update, or replacement of the at least one of the one or more device agents is associated with a credential that is consistent with (e.g., matches) the agent credential.

[0063] In some embodiments, the agent credential comprises one or more of agent kernel software present with a proper signature, certificate, or hash result; agent framework software present with a proper signature, certificate, or hash result; and agent application software present with a proper signature, certificate, or hash result.

[0064] In some embodiments, the end-user device is further secured by configuring the one or more device agents to perform one or more of the following checks: determining if a hosts file is present and properly configured; determining if a service processor on the end-user device successfully completed an authentication procedure with a service controller in the network; determining if the end-user device has been rooted.

[0065] In some embodiments, a network system is configured to provide access network services to an end-user device, and the end-user device is responsible for implementing an access network policy. In some embodiments, the network system is configured to obtain a trusted measure of access network usage by the end-user device and to use the trusted measure to confirm that the end-user device is properly implementing the access network policy, where the trusted measure is obtained from a network element, from a secure processor on the end-user device, or from a trusted third party.

[0066] In some embodiments, the network system is configured to apply a multi-tiered policy verification process comprising at least two of the following policy

IPR2025-01572
Apple EX1002 Page 23

verification steps, performed in any order: (a) determining if the end-user device is failing to send service usage reports, even though the network system is receiving trusted reports of the end-user device's service usage; (b) comparing a trusted service usage measure to a limit or range of usage expected if the end-user device is properly implementing the access network policy; (c) comparing a trusted service usage measure to a non-secure (e.g., device-generated) usage measure to determine if the difference between the two usage measures is within a specified tolerance; (d) comparing a non-secure (e.g., device-based) service usage measure to a limit or range of usage expected if the end-user device is properly implementing the access network policy; (e) comparing a classification of the end-user device's usage to a limit or range of usage expected if the end-user device is properly implementing the access network policy; (f) comparing an aggregation of two or more classifications of the end-user device's usage to an aggregate limit on usage to determine if the difference between the two measures is within a specified tolerance; (g) comparing a trusted measure of usage of a class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) to a limit or range of usage expected if the end-user device is properly implementing the access network policy; (h) comparing a trusted measure of usage of a class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) to a non-secure (e.g., device-based) measure of usage of the same class to determine if the difference between the two measures is within a specified tolerance; (i) comparing a statistical characterization of usage by a population of end-user devices to a trusted measure of the end-user device's service usage to determine if the difference between the two measures is within a specified tolerance; (j) comparing a statistical characterization of usage of a particular class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) by a population of end-user devices to a trusted measure of the end-user device's usage of that same class to determine if the difference between the two measures is within a specified tolerance; (k) comparing a statistical characterization of usage by a population of end-user devices to a non-secure measure of the end-user device's service usage to determine if the difference between the two measures is within a specified tolerance; (l) comparing a statistical characterization of usage of a class (e.g., an application, a group of

IPR2025-01572
Apple EX1002 Page 24

applications, a network destination, a group of network destinations, etc.) to a non-secure (e.g., device-based) measure of usage of the same class to determine if the difference between the two measures is within a specified tolerance; (m) comparing detailed class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) usage information in a usage report (trusted or non-secure) to determine whether the access network policy allows the classified activity; (n) determining whether a service processor on the end-user device successfully authenticated with a service controller in the network; (o) determining whether the end-user device is sending reports to a network element in an expected manner; (p) determining whether usage of one or more classes (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) is consistently slightly under particular limits that would indicate likely fraud on the part of the end-user device; (q) comparing an amount or percentage of unknown or unclassified data usage allocated by the end-user device to a particular class to an expected amount or percentage of unknown or unclassified data usage, where the expected amount or percentage is determined using information from a trusted source (e.g., a web crawler, domain object model, etc.).

[0067] In some embodiments, the result of one or more of the policy verification steps is a pass/fail criterion, and the overall pass criterion is a number of failures less than a limit on the number of failures. In some embodiments, the result of one or more of the policy verification steps is a quantized value associated with an error likelihood or non-error likelihood, and the overall fail/pass criterion is based on a combination of one or more quantized values. In some embodiments, a policy implementation error action is taken if an error occurs, where the error action comprises one or more of: flagging the end-user device or the user for further evaluation; charging for the end-user device's usage at a pre-defined rate associated with an error condition; notifying the user of the end-user device; notifying a network or system administrator; quarantining the end-user device or a user access to the access network; suspending the end-user device or user's access to the access network.

IPR2025-01572
Apple EX1002 Page 25

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] Figure 1 illustrates, at a high level, the various components of a device-assisted services (DAS) implementation in accordance with some embodiments. Service processor 115 resides on an end-user device (not shown) and communicates with service controller 122, which, in the embodiment of Figure 1, resides in the cloud. As will be described below, service processor 115 and service controller 122 communicate over an

IPR2025-01572
Apple EX1002 Page 26

access network to facilitate providing device-assisted services.

[0071] As illustrated in the embodiment of Figure 1, service controller 122 communicates with existing network, information technology (IT), and billing infrastructure 14 of the network operator in various ways that are described herein and in the applications listed in the section "Cross Reference to Related Applications." Service design center 20 provides an interface that allows operator personnel or other authorized persons to configure service plan information for end-user devices. Service design center 20 communicates with service controller 122, which in turn assists in provisioning service plans by communicating with existing network, IT, and billing infrastructure 14 and service processor 115.

[0072] Figure 2 illustrates an example embodiment of a device-based service processor system in communication with a network-based service controller system. End-user device 100 includes service processor 115. Service processor 115 is responsible for identifying access network communication activity by end-user device 100 and applying an access service policy to govern the communication activity. The communication activity in general comprises end-user device 100's use of or attempted use of access network 10 for data communications to or from, for example, Internet 12.

[0073] In some embodiments, service processor 115 assists in classifying service usage by end-user device 100 into sub-categories (e.g., classes) for the purpose of assisting in usage accounting policy enforcement, access control policy enforcement, applying service usage limits, or notification policy enforcement that differs according to the category (or class). In some embodiments, the classification can be for one or more device applications (e.g., a class comprises one or more application programs). In some embodiments the classification can be for one or more network destinations (e.g., a class comprises one or more network destinations). In some embodiments the classification can be for one or more network types (e.g., a class comprises one or more network types). In some embodiments a classification of service usage referred to as a sponsored service (or an ambient service) can be performed to facilitate allocating access network costs, in whole or in part, associated with the sponsored service to a service sponsor, the service

IPR2025-01572
Apple EX1002 Page 27

sponsor being an entity other than the user or subscriber associated with end-user device 100.

[0074] In some embodiments, the communication activity is classified for purposes of access policy enforcement by service processor 115, or by a network element, based on one or more network destinations associated with the communication activity, such as, for example, a collection of one or more of: a network address, a domain, a URL, a website, a WAP site, a server configured to communicate with a device application, a content distribution site, a network tunnel or tunnel server (such as, for example, a VPN, APN, or other tunnel), a network gateway, or a proxy server. In some embodiments, the communications activity is classified for the purposes of network access policy enforcement by service processor 115 or by a network element based on a collection of one or more device application programs or device operating system (OS) components participating in the communications activity.

[0075] Service processor 115 comprises one or more software or firmware programs that execute on end-user device 100. To aid in disclosure of the invention, service processor 115 is explained using the functional elements or agents shown in Figure 2. The specific allocation of functional elements within service processor 115 can take many forms, and the form presented in Figure 2 is intended to illustrate basic elements but is not intended to be an exhaustive or limiting description of possible functional breakdowns of service processor 115.

[0076] Figure 2 shows several device application programs. TCP application 1604, IP application 1605, and voice application 1602 are shown in Figure 2, but other application programs may be present in addition or instead. Each of these applications is in general initiated by user interaction with end-user device 100, generally through user interface 1697. In the embodiment of Figure 2, data path processing elements of service processor 115 include application interface agent 1693, policy implementation agent 1690, modem selection and control 1811, and several access network modem drivers (dial/DSL modem driver 1831, Ethernet modem driver 1815, WPAN modem driver 1814, WLAN modem driver 1813, and WWAN modem driver 1812).

IPR2025-01572
Apple EX1002 Page 28

[0077] In some embodiments, application interface agent 1693 monitors device application-layer communication activity to identify attempted or successful access network communication activity. In some embodiments, application interface agent 1693 monitors application layer access network communication activity to identify and classify the access network communication activity. In some embodiments, the monitoring of access network communication activity by application interface agent 1693 is reported to service monitor agent 1696. In some embodiments, the monitoring of access communications activity by application interface agent 1693 comprises classifying data traffic flows based on inspection and characterization of which application (e.g., TCP application 1604, IP application 1605, voice application 1602, or any other application on end-user device 100) each flow is associated with. In some embodiments, the monitoring of access communications activity by application interface agent 1693 comprises classifying data traffic flows based on inspection and characterization of which network destination each flow is associated with.

[0078] In some embodiments, service monitor agent 1696, application interface agent 1693, and/or other agents implement virtual traffic tagging by tracking or tracing packet flows through 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.

[0079] In some embodiments, application interface agent 1693 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 to 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

IPR2025-01572
Apple EX1002 Page 29

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 115 hardware and/or software in a manner that is compatible with service controller 122 specifications and the products of other device or service product developers.

[0080] In some embodiments, an agent or combination of agents uses tags to assist in applying a policy (e.g., a notification, charging, or control policy) when an application program on end-user device 100 initiates communications or successfully communicates over an access network. In some such embodiments, the agent or combination of agents determines when an application program initiates or attempts to initiate a communication over the first wireless access network by: identifying a data flow comprising one or more related data transfers or attempted data transfers associated with the application program; assigning a flow tag to the data flow, where the flow tag is a traffic flow identifier; monitoring an access network service usage or attempted service usage associated with the flow tag; and, after identifying the data flow, applying the

IPR2025-01572
Apple EX1002 Page 30

policy to the first wireless access network service usage or attempted service usage associated with the flow tag. As will be appreciated by a person having ordinary skill in the art, the steps of identifying, assigning, and monitoring can occur in any order.

[0081] In some embodiments, application interface agent 1693 applies, implements, or enforces service usage accounting or charging policy for application layer access network communication activity. In some embodiments, this policy implementation function is used to apply, implement, or enforce service usage accounting or charging policy that varies with the classification of the access communication activity as discussed above.

[0082] In some embodiments, application interface agent 1693 implements traffic control policy for application layer access network communication activity. In some embodiments, application interface agent 1693 implements application-level control policy to allow an application to execute on end-user device 100 or to prevent an application from executing. In some embodiments, application interface agent 1693 implements notification policy for application layer access network communication activity.

[0083] In some embodiments, application interface agent 1693 provides applications with an access network service application interface so that the application (e.g., TCP application 1604, IP application 1605, voice application 1602, etc.) can request or provision special access network service permissions such as, for example, an access network quality-of-service (QoS) channel class, a background service usage class, a service usage accounting particular to an application or application class, or a sponsored service usage particular to an application or application class, wherein a sponsor entity other than a user of the end-user device subsidizes an access network usage cost associated with the application or application class. In such embodiments, application interface agent 1693 can communicate with a counterpart in the access network to provide for provisioning of the special access network service permissions for a particular application or class of applications.

[0084] In some embodiments, application interface agent 1693 interacts with

IPR2025-01572
Apple EX1002 Page 31

application programs (e.g., TCP application 1604, IP application 1605, voice application 1602, or another application on end-user device 100) to arrange application settings to aid in implementing application-level service policy implementation or billing. In some embodiments, application interface agent 1693 arranges an application setting by posting, sending, or otherwise communicating a message comprising a setting configuration. In some embodiments, the application setting assists in traffic control (e.g., allow, block, throttle, rate-limit, transmit on a particular network, background traffic control, etc.), notification (e.g., to a user of end-user device 100, to a network element such as service controller 122, etc.), or charging (e.g., to account for usage of access network resources by end-user device 100).

[0085] In some embodiments, application interface agent 1693 interacts with an application program stored on end-user device 100 and configured to access a data service over an access network. In some such embodiments, the application program has an associated policy (e.g., a notification [e.g., of an amount or cost of access network usage associated with the application program, an amount or cost of access network usage associated with the application program over a particular (possibly user-selected) period of time, background or foreground data usage information, etc.], charging, or control policy) to be applied when the application program initiates or attempts to initiate communications over the first access network, and application interface agent 1693 (or another agent on end-user device 100) assists in policy implementation by arranging a setting of the application program by posting, sending, or otherwise communicating the setting to the application program.

[0086] In some embodiments, one or more agents on end-user device 100 are configured to prevent unauthorized modifications, updates, or replacements of the application software by: detecting an attempted installation of update software on end-user device 100, where the update software purports to be a modification, update, or replacement of the application program; obtaining a credential associated with the application program; obtaining a credential associated with the update software; and allowing the update software to be installed on end-user device 100 if the credential associated with the purported modification, update, or replacement of the application

IPR2025-01572
Apple EX1002 Page 32

program matches the credential associated with the application program.

[0087] In some embodiments, application interface agent 1693 is associated with or comprises a credential, and another agent on end-user device 100 (e.g., access control integrity agent 1694, policy control agent 1692, etc.) is configured to prevent unauthorized modifications, updates, or replacements of application interface agent 1693. In some embodiments, the other agent detects an attempted installation of software purporting to be a modification, update, or replacement of application interface agent 1693, obtains the credential associated with application interface agent 1693, obtains a credential associated with the software purporting to be a modification, update, or replacement of application interface agent 1693, and allows the software to be installed on end-user device 100 if the credential associated with the software matches the credential associated with application interface agent 1693.

[0088] In some embodiments, 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, 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, application interface agent 1693 performs a transaction billing intercept function to aid the billing agent 1695 in transaction billing. In some embodiments, application interface agent 1693 transmits or receives a billing test element to aid in verifying transaction billing or service billing.

[0089] In some embodiments, policy implementation agent 1690 monitors device network traffic layer communication activity to identify attempted or successful access network communication activity. In some embodiments, policy implementation agent 1690 monitors network traffic layer communication activity to identify and classify the access communication activity. In some embodiments, the monitoring of access network communications activity by policy implementation agent 1690 is reported to service monitor agent 1696. Traffic layer communication monitoring can be conducted at one or more layers between the application layer (generally referred to as layer 7) and the access

IPR2025-01572
Apple EX1002 Page 33

network media access control layer (generally referred to as layer 2). In some embodiments, traffic layer communication monitoring comprises classifying data traffic flows based on inspection and characterization of layer 7 communication traffic parameters (for example, one or more of application program identifier or credential, network destination classifiers, communication protocol parameters, communication content classifiers, or secure communication protocol parameters such as SSL or TLS connection parameters) and associating the classification with one or more resulting traffic flows, socket flows, or packet flows. In some embodiments, traffic layer communication monitoring comprises classifying data traffic flows based on inspection and characterization of layer 4 communication traffic parameters such as, for example, socket flow tuples. In some embodiments, traffic layer communication monitoring comprises classifying data traffic flows based on inspection and characterization of layer 3 communication traffic parameters (for example, IP addresses). In some embodiments, traffic layer communication monitoring comprises classifying data traffic flows based on inspection and characterization of VPN tunnel parameters, APN tunnel parameters, etc.

[0090] In some embodiments, policy implementation agent 1690 applies, implements, or enforces access network policy at one or more of the communications traffic layers of a device operating system. As discussed above, in some embodiments access network policy can be applied at one or more traffic layers. Traffic layer policy enforcement can be applied at any layer(s) between and including the application layer (generally referred to as layer 7) and the access network media access control layer (generally referred to as layer 2).

[0091] In some embodiments, communications traffic layer policy application comprises policy applied to a classification of data traffic flows based on inspection and characterization of layer 7 communication traffic parameters (for example, one or more of application program identifier or credential, network destination classifiers, communication protocol parameters, communication content classifiers, or secure communication protocol parameters such as SSL or TLS connection parameters) and associating the classification with one or more resulting traffic flows, socket flows, or packet flows. In some embodiments, communications traffic layer policy application

IPR2025-01572
Apple EX1002 Page 34

comprises policy applied to a classification of data traffic flows based on inspection and characterization of layer 4 communication traffic parameters such as, for example, socket flow tuples. In some embodiments, communications traffic layer policy application comprises policy applied to a classification of data traffic flows based on inspection and characterization of layer 3 communication traffic parameters (e.g., IP addresses). In some embodiments, communications traffic layer policy application comprises policy applied to a classification of data traffic flows based on inspection and characterization of VPN tunnel parameters, APN tunnel parameters, etc.

[0092] Connection manager 1804 determines which access network the device is connected to and provides this information to other agents on end-user device 100. In some embodiments, connection manager 1804 also chooses a network connection based on available network connections and a network selection policy instruction from policy control agent 1692.

[0093] Service monitor agent 1696 is responsible for accounting and reporting the access network service usage for end-user device 100. In some embodiments, the service monitoring (e.g., a measure of the access network service usage) is reported to a user of end-user device 100. In some embodiments, the service monitoring is reported to a network element. In some embodiments, the access network service usage is classified by an application breakdown indicating the amount of service usage attributed to one or more applications. In some embodiments, the access network service usage is classified by a network destination or network service breakdown indicating the amount of service usage attributed to one or more network destinations or network services. In some embodiments, the access network service usage is classified by a network type breakdown indicating the amount of service usage attributed to one or more network types. In some embodiments, the network type breakdown includes a roaming network. In some embodiments, the network type breakdown includes a cellular network (e.g., 2G, 3G, 4G, etc.).

[0094] Policy control agent 1692 is responsible for monitoring application layer activity or traffic communication layer activity to identify conditions in which a network

IPR2025-01572
Apple EX1002 Page 35

access policy should be implemented, and then causing a policy enforcement agent (for example application interface agent 1693 or policy implementation agent 1690) to apply the policy. In some embodiments, policy control agent 1692 receives information about an end-user device connection state from other device agents (e.g., connection manager 1804, one of modem drivers 1831, 1815, 1814, 1813, 1812, modem selection and control 1811, an operating system function, etc.) to aid in determining the access network policy settings that should be applied at a given time. For example, without limitation, device connection state information can comprise one or more of application classification information, network destination identifier information, network service identifier information, type of network information, time of day or day of week information, and geographic location information.

[0095] The access network policy instruction provided by policy control agent 1692 to a policy enforcement agent (for example, application interface agent 1693 or policy implementation agent 1690) can comprise a service usage accounting or charging policy in which the service usage is accounted and reported for the purpose of access network service usage accounting or billing. In some embodiments, the service usage is accounted to or billed to a device account or device user account. In some embodiments, the service usage accounting is accounted to or billed to a service sponsor account, where the service sponsor is an entity that is not the device user or a subscriber associated with end-user device 100. In some embodiments, the service usage accounting or charging policy includes modifications in accounting policy based on one or more classifications of service usage and one or more device connection states, with classifications of service usage and connection state including but not limited to those disclosed herein.

[0096] The access network policy instruction provided by policy control agent 1692 to a policy enforcement agent can comprise a service usage control policy wherein the service usage is governed, limited, or regulated according to a service plan policy. In some embodiments, the service usage control policy includes modifications in control policy based on one or more classifications of service usage and one or more device connection states, with classifications of service usage and connection state including but not limited to those disclosed herein.

[0097] The access network policy instruction provided by policy control agent 1692 to a policy enforcement agent can comprise a service notification policy in which a notification associated with the access network service is presented through a user interface of end-user device 100 (e.g., user interface 1697) when a pre-determined notification trigger condition is met. In some embodiments, the notification indicates an amount of service used. In some embodiments, the notification indicates an amount of service remaining. In some embodiments, the notification comprises an offer to acquire service. In some embodiments, the service notification policy includes modifications in control policy based on one or more classifications of service usage and one or more device connection states, with classifications of service usage and connection state including but not limited to those disclosed herein. In some embodiments, the notification includes an offer to acquire service based on the occurrence of a pre-determined attempted or successful device access to an application or combination of applications. In some embodiments, an offer to acquire service is based on the occurrence of a pre-determined attempted or successful device access to a network destination or combination of network destinations. In some embodiments, an offer to acquire service is based on detection of a condition in which a new service plan may be of interest to a device user who currently has an existing service plan or no service plan. In some embodiments, the notification comprises an offer to increase a service allowance. In some embodiments, the notification comprises an indication of potential or likely service usage. In some embodiments, the notification indicates a roaming service usage. In some embodiments, the notification comprises an offer to acquire roaming services. In some embodiments, the notification indicates that service authorization is about to expire under a current service plan.

[0098] In some embodiments, user interface 1697 provides a user of end-user device 100 with input capability to modify an access network service according to a user preference and/or to receive access network service notifications. In some embodiments, user interface 1697 accepts user inputs for modifying access network policy, such as limiting access by one or more applications or access to one or more network destinations. In some embodiments, user interface 1697 accepts user inputs for

IPR2025-01572
Apple EX1002 Page 37

modifying end-user device 100's access to particular access networks (e.g., one or more roaming networks, one or more cellular networks, one or more WiFi networks, etc.). In some embodiments, user interface 1697 accepts user inputs for choosing or modifying a service plan.

[0099] Service control device link 1691 provides a secure communication link and heartbeat function between service processor 115 and service controller 122. In some embodiments, using the heartbeat function, agents on end-user device 100 provide certain reports to service controller 122 for the purpose of service policy implementation verification (e.g., verification-related reports on certain aspects of service processor 115) or for other purposes. Such agent heartbeat messages can be sent unencrypted or encrypted, signed, or otherwise secured. In some embodiments, these messages include one or more of an agent information message, an agent check-in message, and an agent cross check message.

[00100] In some embodiments, an agent information message is included in a agent heartbeat service policy implementation verification message, which includes, for example, any information the agent needs to communicate to 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.

[00101] 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).

[00102] In some embodiments, an agent cross-check message is included in the

IPR2025-01572
Apple EX1002 Page 38

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 service processor 115, and/or other messages regarding the verification or possibility of compromise associated with service processor 115 operating environment or agents.

[00103] 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 are transmitted to end-user 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 associated with one or more applications or one or more network destinations 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.

[00104] In some embodiments of the heartbeat function, service controller 122 verifies that the scheduled agent reports are being received and that the reports are within expected parameters. In some embodiments, access control integrity server 1654 issues signed challenge/response sequences to policy implementation agent 1690. For example, the challenges can be asynchronous, issued when an event or error condition occurs,

IPR2025-01572
Apple EX1002 Page 39

issued on a schedule, or issued when a certain amount of data has been used. 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.

[00105] In some embodiments, the challenge/response heartbeat message can include sending any kind of command or query, transmitted securely 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 would be difficult for the agent to supply 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 would be difficult for the agent to supply if the agent were not properly configured, not operating properly, partially compromised, or entirely compromised. In some embodiments, a first agent is required to respond back with information regarding the operation, configuration, status or behavior of a second agent, and this information is difficult for the first or second agent to supply 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 of portions of code or a code sample (e.g., the code portion or code sample can be specified by service controller 122).

[00106] In some embodiments, the information the agent responds with is a

IPR2025-01572
Apple EX1002 Page 40

response to a signed or encrypted message from service controller 122, and 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 for the agent to respond correctly, and for service controller 122 to decode the message, 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 service controller 122. 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.

[00107] 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 (e.g., fraud). There are many other functions the agent heartbeat service can perform; some are described herein, and others will be apparent to one of ordinary skill in the art given the principles, design background, and various embodiments provided herein.

[00108] In some embodiments, service downloader 1663 provides for one or more of: download of application programs that have an associated service policy; download of application credentials; and download of service processor 115 components or component updates. In some embodiments, service downloader 1663 requires a secure signed version of software before a download is accepted. For example, the download can require a unique key or credential. In some embodiments, service downloader 1663

IPR2025-01572
Apple EX1002 Page 41

is stored or executed in secure memory or executes in 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 service downloader 1663.

[00109] Access control integrity agent 1694 monitors the operational integrity of one or more service processor 115 elements to determine if unauthorized user modification or unauthorized user software program modification of the service processor configuration or operation has occurred. In some embodiments, access control integrity agent 1694 collects device information on one or more of service policy, service usage, service activity, agent configuration, and agent behavior. In some embodiments, 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, access control integrity agent 1694 initiates action when a service policy violation or a system integrity breach is suspected. In some embodiments, access control integrity agent 1694 takes an action (e.g., generating a fraud alert, blocking end-user device 100 from accessing access network 10, blocking an application from accessing access network 10, directing the device to a quarantine network status in which end-user device 100 can, for example, only access functions generally controlled by the access network service provider or the central service provider, etc.) when unauthorized conditions are detected. In some embodiments, access control integrity agent 1694 also performs asynchronous or periodic agent checks to verify the presence, configuration, or proper operation of other agents. In some embodiments, access control integrity agent 1694 also performs challenge-response sequence verification of other agents.

[00110] In some embodiments, access control integrity agent 1694 monitors agent self-check reports to verify that agents are properly configured. In some embodiments, access control integrity agent 1694 reports the agent self check reports to service controller 122. In some embodiments, 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, access control integrity agent 1694 performs a role in billing test

IPR2025-01572
Apple EX1002 Page 42

event generation and/or monitoring. In some embodiments, 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.

[00111] In some embodiments, access control integrity agent 1694 receives agent access attempt reports to determine if unauthorized agent access attempts are occurring. In some embodiments, access control integrity agent 1694 acts as a central secure communications hub for agent-to-agent or service-controller-to-agent communication. For example, access control integrity agent 1694 can be used so that no other software or function can access agents or so that agents cannot access other agents except through a 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-to-agent communications, and possibly including unauthorized attempts to communicate 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 service controller 122 requests the agent communication trace log or when there is a verification error event.

[00112] In some embodiments, access control integrity agent 1694 obtains service usage or service activity measures from 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.

[00113] As illustrated in the embodiment of Figure 2, service processor 115 is in communication with service controller 122 via access network 10 (and optionally including an additional connection path via Internet 12 in embodiments in which service controller 122 is not directly connected to access network 10, such as the embodiment of Figure 2). Service controller 122 includes service control server link 1638, which provides a secure communication link and heartbeat function between service processor

IPR2025-01572
Apple EX1002 Page 43

115 and service controller 122.

[00114] In some embodiments, service history server 1650 records service usage reports for end-user device 100. In some embodiments, service history server 1650 collects and records service usage or service activity reports (e.g., accounting reports) from a network element (e.g., access network AAA server 1621) or end-user device 100 (e.g., service monitor agent 1696). In some embodiments, the service usage reports are generated by service processor 115. In some embodiments, the service usage reports include service usage classification information (e.g., usage per application, per group of applications, per network destination, per group of applications, per network type, etc.) as described herein.

[00115] Although service usage reports from the network elements can in certain embodiments be less detailed than service usage reports from end-user device 100, the reports from the network can provide a valuable source for verification of device service policy implementation, because, for example, it is unlikely that a device error or compromise event on end-user device 100 will compromise network-based equipment or software. In some embodiments, service history server 1650 provides the service history on request to other servers and/or one or more agents. In some embodiments, service history server 1650 provides the service usage history to device service history 1618.

[00116] In some embodiments, policy management server 1652 includes storage of access network service policies that are provided to service processor 115 from a network element. In some embodiments, policy management server 1652 provides known-application credentials to service processor 115. In some embodiments, policy management server 1652 evaluates run-time application credentials provided by service processor 115.

[00117] In some embodiments, policy management server 1652 transmits policies to service processor 115 via service control link 1653. In some embodiments, policy management server 1652 manages policy settings on end-user device 100 (e.g., various policy settings as described herein with respect to various embodiments) in accordance with a device service profile. In some embodiments, policy management server 1652 sets

IPR2025-01572
Apple EX1002 Page 44

instantaneous policies on policy implementation agents (e.g., policy implementation agent 1690). For example, policy management server 1652 can issue policy settings, monitor service usage and, if necessary, modify policy settings.

[00118] In some embodiments, policy management server 1652 provides adaptive policy management on end-user device 100. For example, policy management server 1652 can issue policy settings and objectives and rely on the device-based policy management (e.g., by service processor 115) for some or all of the policy adaptation. This approach can require less interaction with end-user device 100, thereby reducing network chatter on service control link 1653 for purposes of device policy management. 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, policy management server 1652 adjusts service policy based on time of day. In some embodiments, 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.

[00119] In some embodiments, policy management server 1652 performs a service control algorithm to assist in managing overall network capacity or application QoS. In some embodiments, 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.

[00120] In some embodiments, access control integrity server 1654 monitors the integrity of the access policy system to establish a trusted service policy implementation. In some embodiments, access control integrity server 1654 collects end-user device 100 information on service policy, service usage, agent configuration and/or agent behavior. In some embodiments, access control integrity server 1654 cross-checks this information to identify integrity breaches in the service policy implementation and control system.

[00121] In some embodiments, access control integrity server 1654 initiates action

IPR2025-01572
Apple EX1002 Page 45

when a service policy violation or a system integrity breach or error is suspected or detected. In some embodiments, access control integrity server 1654 (and/or some other agent of service controller 122) acts on access control integrity agent reports and error conditions. In some embodiments, checks performed by access control integrity agent 1654 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.

[00122] In some embodiments, 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 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 that is associated with a particular application or group of applications, data passed that is associated with a particular network destination or group of network destinations, data passed in a period of time, IP addresses, data per IP address, data per network, data per network type, and/or other measures (such as location, downloads, email accessed, URLs, etc.), and comparing such measures to expected service usage behavior given the policies that are supposed to be in place.

[00123] In some embodiments, 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 sponsored 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 stopping at limit without re-up/revising service policy); unauthorized network address; unauthorized service usage (e.g., VOIP, email, and/or web browsing when not authorized); unauthorized application usage (e.g., email, VOIP, email, and/or web when not authorized); 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

IPR2025-01572
Apple EX1002 Page 46

policy.

[00124] In some embodiments, 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.

[00125] In some embodiments, 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). As another example, the user can also be connected to communicate with service support of the service provider regarding

IPR2025-01572
Apple EX1002 Page 47

such reported activities (e.g., by text/chat, voice/phone, and/or video conference to a service support). Accordingly, in some embodiments, access control integrity server 1654 (and/or some other agent of service controller 122) provides a policy/service control integrity service to verify (e.g., periodically and/or based on trigger events) that the service control of the device has not been compromised and/or is not behaving out of policy.

[00126] In some embodiments, upon detection of one or more service verification errors, such as the various service verification errors discussed above, end-user device 100 is directed to a quarantine network status in which end-user device 100 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. In some embodiments, end-user device 100 is completely suspended from the network. In some embodiments, end-user device 100's network access, service capabilities and/or traffic shaping are limited, partially restricted or completely restricted. 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.

[00127] In some embodiments, service download control server 1660 provides for one or more of: download of application programs that have an associated service policy; download of application credentials; and download of service processor 115 components or component updates.

[00128] In some embodiments, billing event server 1662 provides for billing of access network service usage. In some embodiments, the billing is modified based on one or more of the classifications of access network service usage described herein. In some embodiments, the billing is modified based on one or more of the device connection state conditions described herein.

[00129] In some embodiments, device service history 1618 provides trusted (e.g., network-based, third-party-based, or certain device-based) service usage measures for

IPR2025-01572
Apple EX1002 Page 48

billing purposes or for the purpose of verifying a trusted service policy implementation. In some embodiments, a trusted service policy implementation is verified by service controller 122 (e.g., access control integrity server 1654) by comparing the trusted service usage records with the usage limitations expected to be in place if the service policy is being properly implemented by end-user device 100. In some embodiments, these trusted service usage measures include a classification of service usage based on application. In some embodiments, these trusted service usage measures include a classification of service usage based on network destination or network service identifier. In some embodiments, these trusted service usage measures include a classification of service usage based on network type. In some embodiments, these trusted service usage measures include a classification of service usage based on time of day. In some embodiments, these trusted service usage measures include a classification of service usage based on QoS class. In some embodiments, these trusted service usage measures include a classification of service usage based on geography. In some embodiments, these trusted service usage measures include a classification of service usage based on a roaming network.

[00130] In some embodiments, central billing 1619 provides for billing of service usage. In some embodiments, central billing 1619 provides a mediation function for central provider billing events. For example, central billing 1619 can accept service plan changes. In some embodiments, central billing 1619 provides updates on device service usage, service plan limits and/or service policies. In some embodiments, central billing 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 end-user device 100.

[00131] In some embodiments, access network AAA server 1621 assists in authentication of service processor 115 by providing one or more of a device credential database, a user credential database, a service processor credential database, and an authentication service for the device. In some embodiments, 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 end-user devices 100 onto

IPR2025-01572
Apple EX1002 Page 49

the central provider access network and the service provider network. In some embodiments, 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 service controller 122. In some embodiments, 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, access network AAA server 1621 also records and reports device network service usage (e.g., to device service history 1618).

[00132] Although many of the embodiments disclosed herein include service controller 122, a service controller is not necessary in embodiments in which a user of end-user device 100 is in full control of access network policies via user interface 1697. For example, the user can determine access network service policies that limit service for end-user device 100 in general or for one or more of the access network service usage classifications described herein, including application limitations, network destination or network service limitations, network type limitations, etc. In some embodiments, based solely on user preferences input via user interface 1697 of end-user device 100, the service processor access network service policy limitations can specify blocking, allowing, or capping service usage according to, for example, application, application class, or destination. In some embodiments, these user-defined limitations can be modified based on the type of network the device is connected to. In some embodiments, these user defined limitations can be modified based on whether the user wishes to allow the access network communication activity for a given classification to occur in the background or not, or to cap such service usage when end-user device 100 is connected to a particular network type (e.g., a roaming network, a cellular network, a WiFi network, etc.). In some embodiments, these user-defined limitations can be modified based on whether the user wishes to allow the access network communication activity for a given classification to occur while end-user device 100 is connected to a roaming network, or to cap such service usage while end-user device 100 is roaming.

[00133] Figure 3 illustrates an alternative embodiment of functional elements for a network access service policy implementation. In Figure 3, the carrier network system is

IPR2025-01572
Apple EX1002 Page 50

shown as having multiple radio access networks (RAN 1657 and RAN 1659 are shown, but additional networks may also be present), carrier core gateways 1656, carrier core network usage monitors 640, carrier network 11, and carrier billing 139. In this embodiment, the service controller function is augmented by authentication credential server 220, application credential data base 221, application policy database 223, service usage reconciliation and fraud detection 642, and service design center 20. In some embodiments, authentication credential server 220 is incorporated in service controller 122.

[00134] Internet 12 provides a connection to user device application program sources (e.g., third-party app stores 500) and user device application service destinations (e.g., app developer servers 600 and other websites, servers, or content sources connected to Internet 12). Application developer service design center (SDC) user interface (UI) 610 provides a user interface to allow application developers or website developers who choose to sponsor (e.g., partially or entirely subsidize) access network usage costs associated with particular applications and/or websites to define sponsored-service parameters. Usage or transaction monitors 620 track device usage of application developer servers 600 (e.g., by generating customer usage or transaction feedback 630) for the purpose of verifying access network service policy for sponsored services.

[00135] Authentication credential server 220 interfaces with application credential database 221, with application policy database 223, and with service controller 122. Authentication credential server 220 has at least three embodiments, each with a different mode of operation. In one embodiment or mode of operation, authentication credential server 220 provides application credentials and associated access network policies to end-user device 100 (e.g., to service processor 115) for the purpose of identifying a device application program and associating it with access network policies that are to be applied to attempted or successful access network communications associated with that application. A device application program credential can be a program identifier, a name, a signature, a certificate, a hash, or any other identifier that uniquely identifies the application. In another embodiment or mode of operation, authentication credential server 220 receives a device application credential from end-user device 100 (e.g.,

IPR2025-01572
Apple EX1002 Page 51

service processor 115), determines if the credential matches a known-application credential in application credential database 221, and, if so, provides the associated application access service policy from application policy database 223 to the device. In a variation of this embodiment, if authentication credential server 220 determines that the application credential does not match a known-application credential in application credential database 221, then, in some embodiments, authentication credential server 220 retrieves an access policy associated with unknown applications from application policy database 223 and provides it to end-user device 100. In some embodiments in which the application credential does not match a known-application credential, end-user device 100 is informed that no policy exists for the application associated with the credential. In some embodiments in which the application credential does not match a known-application credential, no action is taken.

[00136] Carrier core network usage monitors 640 monitor usage of access network resources by each end-user device 100. Carrier core network usage monitors 640 may include a deep packet inspection (DPI) element or any other network element capable of monitoring usage of access network resources by end-user devices.

[00137] Service design center 20 provides a means for specifying service plan policies for the access network service policy implementation system. Co-pending United States patent application number 13/248,025, which is entitled "Service Design Center for Device Assisted Services" and is incorporated herein by reference, describes some of the information that may be configured via service design center 20. Examples of information that can be configured using service design center 20 include but are not limited to: a list of available service plans; the priorities of listed service plans, where the priorities identify the order in which the classification function on the end-user device should apply filters associated with the available, selected, or purchased service plans, e.g., to determine under which plan a particular service activity by an end-user device falls; how available service plans will be displayed on an end-user device, such as end-user device 100; a categorization of service plans (e.g., whether a service plan is a temporary activation plan, a sponsored plan subsidized or paid for by an entity other than a user or subscriber associated with the end-user device, a user-paid plan, etc.);

IPR2025-01572
Apple EX1002 Page 52

promotional messages to be displayed on one or more end-user devices, such as end-user device 100; upsell offers (e.g., conditions that trigger the display of an upsell offer, information characterizing the upsell offer, etc.); events that cause a "no capable plan" notification (e.g., a notification that is presented when a user of an end-user device that is not associated with or subscribed to an applicable data plan attempts to access a data service, etc.) on the end-user device; templates for notification messages (e.g., message foregrounds and backgrounds, colors, logos, etc.); subscriber groups (e.g., by importing a list, manually typing individual subscriber identifiers, etc.); requests for reports containing information about a group of end-user devices or a group of subscribers; information about an end-user device associated with a subscriber (e.g., data usage measures, service plan information, cost or account balance information, notification settings for the end-user device, etc.).

[00138] In some embodiments, service usage reconciliation and fraud detection 642 provides service usage comparisons for the purpose of service fraud detection and corrective action. As disclosed herein, service usage measures used by service usage reconciliation and fraud detection 642 can originate from end-user device service usage measures, trusted service usage measures (e.g., measures from carrier core network usage monitors 640 or another trusted source), or both. As also disclosed herein, the service usage measures can be associated with various classifications (e.g., by application, network destination, device network connection state, network type, etc.). In some embodiments, a trusted service policy implementation is verified by service controller 122 by performing one or more of the following operations: (a) comparing the trusted access network usage records with the usage limitations expected to be in place if the service policy is being properly implemented; (b) comparing a trusted service usage measure against a device service processor-based service usage measure; (c) comparing a first device service processor service usage measure against a second device service processor service usage measure; (d) comparing device service usage against a population statistic for the device-based service usage measure.

[00139] In some embodiments, service usage reconciliation and fraud detection 642 uses customer usage or transaction feedback 630 from usage or transaction monitors

IPR2025-01572
Apple EX1002 Page 53

620 integrated into application developer servers 600 to aid in detection of service policy error events. In some embodiments, the service usage information provided from customer usage or transaction feedback 630 is used to determine the service usage that should be accounted to an application classification service, a website classification service, a network content classification service, or a network classification service defined by a connection to a network gateway, proxy server, or tunnel server (e.g., an APN tunnel server, a VPN tunnel server, etc.). In some embodiments, the service usage provided from customer usage or transaction feedback 630 is compared to device-based service usage measures to determine if the two measures are accurate to within a tolerance.

[00140] In some embodiments, third-party app stores 500 provide end-user device 100 with an application program source for downloading device application programs associated with an access network policy. In some embodiments, when (as disclosed herein) a device user interface notification offers a user a service plan comprising an application program and an associated access network policy for the application program, and the application program is not pre-loaded on the device, when the user selects the service plan, service processor 115 automatically downloads the application from one of third-party app stores 500.

[00141] In some embodiments, application developer service design center UI 610 allows application developers, website developers, or other Internet content providers or service providers to log into a sponsored service definition server in order to sign up for sponsored payments to subsidize user accounting for access network service usage for a certain application, certain website, certain content site, certain shopping site, or another Internet based service associated with a network destination, a group of network destinations, an application, a group of applications, a network type, etc. In some embodiments, an application credential can be uploaded or specified via application developer service design center UI 610 and associated with a sponsored service plan policy. In some embodiments, a network destination identifier can be uploaded or specified via application developer service design center UI 610 and associated with a sponsored service plan policy.

IPR2025-01572
Apple EX1002 Page 54

[00142] In some embodiments carrier billing 139 provides for billing of service usage.

Secure Service Controller Hardware Architectures

[00143] The elements of service controller 122 described herein can be implemented in various advantageous architectural embodiments to assist in securing device-assisted services (DAS). Figure 4 illustrates an example embodiment of a secure service controller architecture for DAS systems. Figure 4 shows several of the functions that may be accomplished by a service controller (e.g., service controller 122) that communicates with one or more end-user devices over access network 10. In particular, Figure 4 shows four service controller functions: a portal function, a file transfer function, a gateway function, and a credentialing function.

[00144] In the embodiment of Figure 4, the portal function is accomplished by portal user 102, optional load balancer 106, optional portal proxy server 108, portal application server 112, and database cluster 116. In some embodiments, the portal function allows a user (e.g., carrier personnel, mobile virtual network operator (MVNO) personnel, virtual service provider (VSP) personnel, etc.) to enter information to configure or manage access network services or end-user devices, such as by using service design center 20 or application developer service design center UI 610. In some embodiments, the portal function allows a portal user to collect information about provisioned end-user devices (e.g., reports containing information about an end-user device's service plan activity, reports containing information about an end-user device's access network usage, etc.). An example embodiment of the portal function is described in more detail below using Figure 9.

[00145] In some embodiments, the file transfer function allows secure file transfers between a carrier (e.g., a service provider, an MVNO, a VSP, etc.) and the service controller. As illustrated in Figure 4, carrier file 118 is placed on file server 126 through optional load balancer 124. EAI server 128 retrieves carrier file 118. In some embodiments, EAI server 128 processes carrier file 118. EAI server 128 configures output file 120. In some embodiments, EAI server 128 configures output file 120 using

IPR2025-01572
Apple EX1002 Page 55

information in database cluster 116. EAI server 128 places output file 120 on file server 126. An example embodiment of the file transfer function is described below using Figure 10.

[00146] In the embodiment of Figure 4, the credentialing function is accomplished by end-user device 100, optional load balancer 142, optional credentialing proxy server 144, credentialing application server 146, and database cluster 116. In some embodiments, the credentialing function authenticates end-user devices and provides those devices with the credentials they need in order to communicate with the service controller gateway and to use access network services. An example embodiment of the credentialing function is described below using the example embodiment of Figure 6.

[00147] In the embodiment of Figure 4, the gateway function is accomplished by end-user device 100, optional load balancer 134, optional gateway proxy server 136, gateway application server 138, and database cluster 116. In some embodiments, the gateway function supports an end-user device's DAS communications, including the sending of device-based usage reports from end-user device 100 (e.g., using service processor 115) to service controller 122, after the end-user device has completed the credentialing procedure. An example embodiment of the gateway function is described below using Figure 11.

[00148] In some service controller 122 embodiments, security is provided by making data flowing through the service controller accessible only to the functions and elements that process it. For example, in the embodiment of Figure 4, information flowing from end-user device 100 to credentialing application server 146 is not available to network elements supporting the portal, file server, or gateway functions. Figure 4 also illustrates several different security zones. The security zones are protected (e.g., separated) by firewalls that limit the reach of an entity once that entity has gained access to a hardware element or function within a hardware element that performs a service controller function. As would be understood by a person of ordinary skill in the art, a firewall comprises one or more devices that permit or deny network traffic to pass through the firewall based on a set of rules. When interposed between two network

IPR2025-01572
Apple EX1002 Page 56

elements, a firewall can prevent unauthorized access between elements while permitting legitimate communications to pass. In the embodiment shown in Figure 4, once an entity has gained access to an element in one security zone, the entity must pass through a firewall to communicate with an entity in a different security zone. For example, firewall 104 protects optional load balancer 106 and portal proxy server 108 from unauthorized access by portal user 102; firewall 110 protects portal application server 112 from unauthorized access by optional portal proxy server 108; and firewall 114 protects database cluster 116 from unauthorized entry by portal application server 112. Thus, in order to gain access to database cluster 116, portal user 102 must successfully navigate through three firewalls.

[00149] Figure 4 illustrates seven security zones, each indicated by a dashed line. The zone labeled "DMZ 1" includes optional load balancer 106 and optional portal proxy server 108. DMZ1 is separated from portal user 102 by firewall 104, and DMZ1 is separated from portal application server 112, which is in the "App VLAN" security zone, by firewall 110. The zone labeled "DMZ 2" includes optional load balancer 124 and file server 126. Incoming carrier file 118 must pass through firewall 18 to reach file server 126, and through firewall 110 to reach EAI server 128. Likewise, retrieving output file 120 from file server 126 requires navigation through firewall 18. The zone labeled "DMZ 3" includes optional load balancer 134 and optional gateway proxy server 136. Communications from end-user device 100 must pass through firewall 132 to reach optional gateway proxy server 136, and through firewall 110 to reach gateway application server 138. The zone labeled "DMZ 4" includes optional load balancer 142 and optional credentialing proxy server 144. Communications from end-user device 100 must pass through firewall 140 to reach credentialing proxy server 144 and through firewall 110 to reach credentialing application server 146. Figure 4 also shows a security zone labeled "Database VLAN," which includes database cluster 116 and is protected from the elements in the App VLAN security zone by firewall 114. Database cluster 116 comprises one or more database elements. The information in and use of database cluster 116 is described below. The zone labeled "DMZ 5" contains carrier IT/billing element 139 and is separated from EAI server 128 and the other elements in the App VLAN zone

IPR2025-01572
Apple EX1002 Page 57

by firewall 235.

[00150] The zone labeled "App VLAN" is the applications security zone. As illustrated in Figure 4, App VLAN includes portal application server 112, EAI server 128, message bus 130, fraud server 129, reconciliation server 131, gateway application server 138, and credentialing application server 146. Figure 4 illustrates direct communication paths between some of the elements within the App VLAN zone. For example, there are direct communication paths between EAI server 128 and portal application server 112; between EAI server 128 and message bus 130; between fraud server 129 and message bus 130; between reconciliation server 131 and message bus 130; and between gateway application server 138 and message bus 130. Figure 4 also shows that several of the elements within the App VLAN security zone do not communicate directly, but rather use message bus 130. For example, there is no direct communication path between EAI server and reconciliation server 131, but both elements have communication paths with message bus 130. As would be appreciated by a person having ordinary skill in the art, elements with communication paths through message bus 130 could have direct communication paths, and elements with direct communication paths could instead communicate using message bus 130. The communication paths shown in Figure 4 are merely exemplary.

[00151] Although Figure 4 shows the various elements within App VLAN as being within a single security zone, a person of ordinary skill in the art would recognize that there may be multiple security zones, separated by firewalls, within the App VLAN zone to provide added security. For example, there could be a firewall between portal application server 112 and EAI server 128. Also, although Figure 4 illustrates separate elements (e.g., portal application server 112, EAI server 128, etc.) within the App VLAN security zone, this representation is merely a functional representation. As would be appreciated by a person having ordinary skill in the art in light of the disclosures herein, some or all of the elements shown may be combined in a single element (e.g., two or more of the illustrated elements could be performed by a single processor, a single server, etc.).

IPR2025-01572
Apple EX1002 Page 58

[00152] Although Figure 4 illustrates credentialing application server 146 as not communicating with any of the other elements within the App VLAN security zone, in some embodiments it may be advantageous for credentialing application server 146 to communicate with other elements in the App VLAN security zone, such as, for example, EAI server 128 or portal application server 112, to assist in tasks such as, for example, preventing a particular end-user device or a particular subscriber from being allocated a credential or revoking the credential of a particular end-user device or a particular subscriber. As another example, in some embodiments, credentialing application server 146 communicates directly with fraud server 129 to flag fraudulent uses of credentials.

[00153] Although Figure 4 illustrates firewalls as separate elements, each physical machine implementing one or more functions or elements shown in Figure 4 could contain its own firewall. Furthermore, each logical element in each layer could be further firewalled beyond what is shown in Figure 4. As an example, the logical elements that only communicate with message bus 130 could be individually firewalled so they are only allowed to send traffic to and receive traffic from message bus 130.

[00154] As illustrated in Figure 4, in addition to communicating with portal application server 112 and message bus 130, EAI server 128 communicates with carrier IT/billing 139 through firewall 235. In this embodiment, EAI server 128 has an interface that allows it to communicate with carrier IT/billing 139. The information flowing to and from EAI server 128 over the various communication paths shown in Figure 4 is described below in more detail using the example embodiment of Figure 7.

[00155] Figure 5 illustrates an example embodiment that is similar to the embodiment of Figure 4, except without the optional load balancers and without the optional proxy servers. As shown in Figure 5, communications from portal user 102 or from end-user device 100 must pass through two firewalls, firewall 110 and firewall 114, to reach database cluster 116. Three firewalls (122, 110, and 114) separate carrier file 118 and database cluster 116. Carrier IT/billing element 139 must pass through firewall 235, EAI server 128, and firewall 114 to reach database cluster 116.

[00156] Figure 6 illustrates an example embodiment without the optional load

IPR2025-01572
Apple EX1002 Page 59

balancers and without the optional proxy servers of Figure 4, and with an external EAI interface between EAI server 128 and carrier IT/billing 139. As illustrated in Figure 6, firewall 237 is interposed between EAI interface 238 and carrier IT/billing 139 to provide additional security, and EAI interface 238 resides in a security zone labeled "DMZ 6." In the embodiment of Figure 6, communications from/to EAI server 128 to/from carrier IT/billing 139 must pass through two firewalls (235 and 237).

[00157] Figure 7 illustrates a more general representation of the communications within the App VLAN security zone illustrated in Figures 1A through 1C. In Figure 7, portal application server 112, credentialing application server 146, gateway application server 138, reconciliation server 131, fraud server 129, and EAI server 128 all communicate using message bus 130. Message bus 130 may be any kind of inter-process communication. Some examples of inter-process communication are: a named pipe, a shared memory, a message queue, a web service call, an IP socket, an remote procedure call (RPC), and a Java messaging services (JMS) queue. Message bus 130 may be multi-functional and simultaneously support multiple types of inter-process communication between the elements shown in Figure 7. Specifically, message bus 130 may support one kind of inter-process communication between one pair of elements shown in Figure 7 and a different kind of inter-process communication between a different pair of elements. For example, message bus 130 might support web service calls for communications between portal application server 112 and EAI server 128, and a message queue for communications between EAI server 128 and fraud server 129.

[00158] Figure 8 illustrates an example embodiment that provides geo-redundancy. For clarity, Figure 8 omits several details present in Figures 1A through 1C, including firewalls. Figure 8 shows service controller 162 and service controller 164. Service controller 162 includes portal function 154, gateway function 158, credentialing function 157, file server function 156, and database cluster 116. Service controller 164 has corresponding functions (portal 168, gateway 172, credentialing 173, and file 170) and database cluster 174. Service controller 162 and service controller 164 are functionally equivalent but physically distinct. In some embodiments, one of service controller 162 and service controller 164 is active (i.e., in use to service portal user 102 and end-user

IPR2025-01572
Apple EX1002 Page 60

device 100, and able to process carrier file 118), and the other service controller is in a stand-by state (e.g., fully functional but not in active use). In some embodiments, both of service controller 162 and service controller 164 are active.

[00159] Portal user 102, end-user device 100, and carrier file 118 access one or both of service controllers 162 and 164 through global load balancer 150, which routes carrier file 118 and communications to and from portal user 102 and end-user device 100. In some embodiments in which both of service controller 162 and service controller 164 are active, global load balancer 150 determines (e.g., based on the level of busyness or outage state of elements within service controller 162 and service controller 164) whether to route a particular communication to service controller 162 (potentially through optional load balancer 152) or to service controller 164 (potentially through optional load balancer 166). In some embodiments in which one of service controller 162 and service controller 164 is active and the other is in a stand-by state, global load balancer 150 routes communications to and from the active service controller unless or until there is a need to use functions in the stand-by service controller (e.g., if one or more elements in the active service controller fail, if the active service controller's ability to service communications becomes compromised for some reason, etc.). The architecture shown in Figure 8 provides reliability in that a failure within either service controller 162 or service controller 164 will not disable the network's ability to provide service controller services to portal user 102, end-user device 100, or carrier usage record 118. If, for example, one or more of the hardware elements responsible for credentialing function 157 in service controller 162 fails, global load balancer 150 can route credentialing requests from end-user device 100 to credentialing function 173 in service controller 164. As will now be understood by a person of ordinary skill in the art in light of this disclosure, additional service controllers may be deployed in a similar manner (e.g., connected to load balancer 150, load balancer 152, or load balancer 166) to provide redundancy and to help ensure service controller resources are available for DAS.

[00160] Figure 9 illustrates an example embodiment of the portal function, such as, for example, portal function 154 or portal function 168 illustrated in Figure 8. Figure 9 illustrates optional load balancer 106 and optional portal proxy server 108, but, as

IPR2025-01572
Apple EX1002 Page 61

described previously, these elements and either firewall 104 or firewall 110 may be omitted. Co-pending United States patent application number 13/248,025, which is entitled "Service Design Center for Device Assisted Services" and is incorporated herein by reference, describes some of the information that portal user 102 could configure for use by portal application server 112. In some embodiments, portal user 102 configures a list of available service plans. In some embodiments, portal user 102 configures the priorities of listed service plans, where the priorities identify the order in which the classification function on the end-user device should apply filters associated with the available, selected, or purchased service plans, e.g., to determine under which plan a particular service activity by an end-user device falls. In some embodiments, portal user 102 enters information pertaining to how available service plans will be displayed on an end-user device, such as end-user device 100. In some embodiments, portal user 102 enters information about a classification of service plans (e.g., whether a service plan is a temporary activation plan, a sponsored plan subsidized or paid for by an entity other than a user of the end-user device, a user-paid plan, etc.). In some embodiments, portal user 102 configures promotional messages to be displayed on one or more end-user devices, such as end-user device 100. In some embodiments, portal user 102 configures upsell offers (e.g., conditions that trigger the display of an upsell offer, information characterizing the upsell offer, etc.). In some embodiments, portal user 102 defines events that cause a "no capable plan" notification (e.g., a notification that is presented when a user of an end-user device that is not associated with or subscribed to a data plan attempts to access a data service, etc.) on the end-user device. In some embodiments, portal user 102 configures templates for notification messages (e.g., message foregrounds and backgrounds, colors, logos, etc.). In some embodiments, portal user 102 creates (e.g., imports a list, manually types individual subscriber identifiers, etc.) or manages (e.g., views, edits, etc.) subscriber groups. In some embodiments, portal user 102 requests reports containing information about a group of end-user devices or a group of subscribers. In some embodiments, portal user 102 is a subscriber (e.g., a person who uses the end-user device), and portal function 154 allows the subscriber to access information about an end-user device associated with the subscriber (e.g., data usage measures, service plan information, cost or account balance information, notification

IPR2025-01572
Apple EX1002 Page 62

settings for the end-user device, etc.). In some embodiments, portal user 102 accesses optional portal proxy server 108 or portal application server 112 using a password. In some embodiments, the password is stored in local storage as a salted SHA-1 hash. In some embodiments, different portal users 102 are given different sets of privileges so that only authorized administrative users can view, enter, or modify particular information, such as, for example, subscriber lists, device lists, etc.

[00161] Portal user 102 accesses optional portal proxy server 108 (if present) through firewall 104 and (if present) optional load balancer 106. In some embodiments, portal user 102 establishes a virtual private network (VPN) connection over the Internet to communicate with optional portal proxy server 108. If present, optional portal proxy server 108 communicates with portal application server 112 through firewall 110.

[00162] As illustrated in Figure 9, portal application server 112 also communicates with EAI server 128. In some embodiments, portal application server 112 sends instructions associated with the delivery of information to end-user device 100 to EAI server 128. In some embodiments, the instructions cause EAI server 128 to configure notification messages (e.g., promotional messages, offers, advertisements, etc.), which EAI server 128 then stores on database 116 for gateway application server 138 to retrieve and send to end-user device 100. In some embodiments, portal application server 112 sends instructions to reset a subscriber or an end-user device to EAI server 128. In some embodiments, portal application server 112 sends instructions to cancel an end-user device service plan to EAI server 128. In some embodiments, portal application server 112 receives messages from EAI server 128 that indicate EAI server 128 carried out a requested task or completed its portion of a requested task that requires action by another network element.

[00163] Portal application server 112 retrieves information from and stores information in database cluster 116 by establishing a connection through firewall 114. In some embodiments, portal application server 112 retrieves information requested by portal user 102 from database cluster 116. In some embodiments, portal application server 112 stores information entered by portal user 102 in database cluster 116.

IPR2025-01572
Apple EX1002 Page 63

[00164] Figure 9 shows three agents that communicate with monitoring element 188. Monitoring element 188 is located in a security zone labeled "Ops VLAN," which is the operations security zone. In some embodiments, the Ops VLAN includes authentication, monitoring, and logging functions. In some embodiments, elements within the Ops VLAN have controlled connectivity to and from the servers shown in Figures 1A through 1C (e.g., portal application server 112, EAI server 128, fraud server 129, reconciliation server 131, gateway application server 138, credentialing application server 146) based on service controller application requirements. As illustrated in Figure 9, portal proxy server 108 includes notification agent 180, which communicates through firewall 186 with monitoring element 188, and portal application server 112 includes notification agent 182 and log forwarder 184, both of which also communicate with monitoring element 188 through firewall 186.

[00165] Notification agent 180 and notification agent 182 provide information to monitoring element 188. In some embodiments, one or both of notification agents 180 and 182 are SNMP agents. In some embodiments, the information provided by one or both of notification agents 180 and 182 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by one or both of notification agents 180 and 182 is in response to a request from monitoring element 188.

[00166] In some embodiments, monitoring element 188 responds to information sent by notification agent 180 or 182. For example, in some embodiments, monitoring element 188 sends notification agent 180 or 182 a message directing (respectively) portal proxy server 108 or portal application server 112 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to determine whether a connected system is functional, etc.). In some embodiments, monitoring element 188 directs portal proxy server to test the communication path to portal application server 112.

[00167] Log forwarder 184 also sends information to monitoring element 188. In some embodiments, log forwarder 184 sends logs of accesses by or activities of portal

IPR2025-01572
Apple EX1002 Page 64

users, such as portal user 102, to monitoring element 188. In some embodiments, portal application server 112 tracks system level commands and login attempts. In some embodiments, log forwarder 184 sends information about system-level commands and login attempts to monitoring element 188. In some embodiments, log forwarder 184 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, portal application server 112 generates log files, and log forwarder 184 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 184 sends a system log, an information log, a debug log, an error log, information about a fatal event, etc. In some embodiments, monitoring element 188 includes a log file harvester. In some embodiments, portal application server 112 initiates the transfer of information from log forwarder 184 to monitoring element 188.

[00168] Figure 10 illustrates an example embodiment of file transfer function 156 (functionally equivalent to file transfer function 170 shown in Figure 8). Carrier file transfer agent 199 establishes a connection with file transfer agent 190 on file server 126 through firewall 18 and optional load balancer 124. The connection enables the transfer of carrier file 118 to file server 126. In some embodiments, carrier file transfer agent 199 establishes a VPN connection over the Internet to communicate with transfer agent 190.

[00169] Carrier file 118 can contain various information, such as, for example: a measure of an access network usage by end-user device 100; information to provision an access network service for one or more end-user devices, such as end-user device 100; a list of end-user devices or subscribers authorized to use a particular service.

[00170] In some embodiments, carrier file 118 comprises a subscriber list. A subscriber list includes one or more subscriber identifiers, where a subscriber identifier is associated with a particular end user. As will be appreciated by a person having ordinary skill in the art, a subscriber identifier may also be associated with a particular end-user device or with a group of end-user devices, or the subscriber identifier may not be associated with any particular end-user device. Examples of subscriber identifiers are: an

IPR2025-01572
Apple EX1002 Page 65

IMSI, an MSID, a MDN, an MSISDN, an MEID, an ESN, an IPv4/6 MAC or IP address, a key, a certificate, a globally unique identifier (GUID), a unique identifier (UID).

[00171] In some embodiments, carrier file 118 includes one or more flow data records (FDRs). A flow data record contains detailed information related to one or more network communications (e.g., source IP, source port, destination IP, destination port, bytes transmitted, bytes received, time flow started, time flow ended, traffic protocol (e.g., TCP/UDP), etc.).

[00172] In some embodiments, carrier file 118 includes a plan catalog that includes information about service plans for the access network that are available to one or more end-user devices. Examples of the information that may be included in a plan catalog are: a list of service plans and their characteristics (e.g., notification, charging, and control policies associated with each plan, access network activities qualifying for each plan, etc.); the priorities of the service plans, where the priorities identify the order in which the classification function on the end-user device should evaluate the filters associated with the available service plans; how the service plans are displayed on end-user devices (e.g., the order in which they are displayed, etc.); whether access network costs associated with a plan are paid by a sponsor entity or by a subscriber; whether a plan is an activation plan (e.g., a service plan that governs a device when a subscriber has not selected a plan); promotional messages; upsell offers; subscriber groups; notifications for which no service plan applies.

[00173] In some embodiments, carrier file 118 includes a list of end-user devices or subscribers authorized to use a particular service (e.g., a tethering service for sharing an access network connection with other devices through other input/output ports on the end-user device).

[00174] In some embodiments, carrier file 118 includes one or more classification rules. A classification rule is any rule that distinguishes between any characteristics of service plans, subscribers, end-user devices, network destinations, or network types. For example, a classification rule may distinguish between sponsor-paid and subscriber-paid service plans, between applications or groups of applications, between groups of

IPR2025-01572
Apple EX1002 Page 66

subscribers, between end-user devices using valid profiles and those using fraudulent profiles, between authorized network destinations and unauthorized destinations, between network access types (e.g., home, roaming, 2G, 3G, WiFi, etc.), between time-of-day rules, etc.

[00175] In the embodiment shown in Figure 10, after being transferred to file server 126, carrier file 118 is transferred to EAI server 128. In some embodiments, the transfer of carrier file 118 to EAI server 128 is initiated by EAI server 128. EAI server 128 processes carrier file 118 and generates output file 120. In some embodiments, EAI server 128 uses information from another source to generate output file 120. In some embodiments, EAI server 128 uses information from carrier file 118 and information from end-user device 100 (e.g., a data usage measure providing information about the end-user device's use of the access network or of a particular service, etc.) to generate output file 120. In some embodiments, EAI server 128 uses information stored in database 116 to generate output file 120. This information can include, for example, individualized or statistical information related to plan usage, popularity of plans, notification acknowledgements, time-of-day usage statistics, average use per plan, subscriber info, subscriber behavior, etc. In some embodiments, EAI server 128 uses information from fraud server 129 to generate output file 120. This information can include, for example, fraud alerts indicating that subscriber service plan usage activity has been detected as abnormal or fraudulent, as well as a confidence score (e.g., to indicate a level of confidence that the user is committing fraud); end-user device fraud events; authentication issues; etc. In some embodiments, EAI server 128 uses information from reconciliation server 131 to generate output file 120. This information can include, for example, detailed or high-level end-user device service usage records, including subscriber identifier, device identifier, service plan identifier, service plan usage (bytes), start time of report, end time of report, etc. In some embodiments, EAI server 128 uses information from gateway application server 138 to generate output file 120. This information can include, for example, information about users, roles, and permissions, or user directory synchronization. In some embodiments, EAI server 128 uses information from portal application server 112 to generate output file 120. This

IPR2025-01572
Apple EX1002 Page 67

information can include, for example, usage reports requested by portal user 102, subscriber data (e.g., provisioning information) import requests from portal user 102, information about accesses by portal users, information about revoked portal user access, etc.

[00176] In some embodiments, output file 120 is a batch report. In some embodiments, output file 120 is a real-time report. In some embodiments, output file 120 includes a measure of an access network usage or cost by an end-user device, such as end-user device 100. In some embodiments, output file 120 is a charging data report (CDR). In some embodiments, output file 120 includes a promotional message or advertisement. In some embodiments, output file 120 includes a subscriber list or an end-user device list. In some embodiments, output file 120 includes information about a service plan purchase made by a user of an end-user device, such as end-user device 100. In some embodiments, output file 120 includes information profiling an end-user device's usage of the access network or of an access network service. In some embodiments, output file 120 includes a fraud alert. A fraud alert is any indication that the service controller or an end-user device has detected activity or an event that suggests that an end-user device may be being used in a manner that violates a policy (e.g., a notification, control, or charging policy) that should be in effect or that the end-user device or device client has been tampered with in a way that compromises the security of the end-user device or an element of the end-user device (e.g., a software application, an agent, an operating system, etc.). A fraud alert may be in any form, for example, a simple flag or a message containing detailed information about the activity or event that caused the fraud alert to issue. A fraud alert can also include information such as, for example, the time the event was detected, the associated subscriber identifier, device identifier, suggested remediation actions, an error code, a rule to be added in the network elements that perform policy charging and rules function (PCRF) or policy charging and enforcement function (PCEF) tasks or to the gateway GPRS support node (GGSN), or any other information that could be useful to understand or mitigate fraudulent activity.

[00177] In some embodiments, EAI server 128 initiates the transfer of output file 120 to file server 126. In some embodiments, the transfer of output file 120 to file server

IPR2025-01572
Apple EX1002 Page 68

126 is initiated by file server 126. In some embodiments, output file transfer agent 203 establishes a connection to file transfer agent 213 to retrieve output file 120. In some embodiments, output file transfer agent 203 establishes a secure connection over the Internet to communicate with file transfer agent 213 through firewall 18. In some embodiments, file server 126 pushes output file 120 to output file transfer agent 203.

[00178] As illustrated in Figure 10, file server 126 also includes notification agent 201, notification agent 196, and file transfer agent 198. Notification agent 201 establishes a connection to message bus 130 through firewall 110. In some embodiments, notification agent 201 places a message for EAI server 128 on message bus 130 to inform EAI server 128 that carrier file 118 is available on file server 126. This notification may be advantageous to increase the speed at which EAI server 128 processes carrier file 118.

[00179] Notification agent 196 provides information to monitoring element 188, communicating through firewall 186. In some embodiments, notification agent 196 is an SNMP agent. In some embodiments, the information provided by notification agent 196 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by notification agent 196 is in response to a request from monitoring element 188.

[00180] File transfer agent 198 provides information to monitoring element 188 through firewall 186. This information can include, for example, file transfer activity, CPU load, disk usage, successful transfers, failed transfers, failed logins, operating environment info (e.g., ambient temperature, humidity, nominal voltage, etc.), system errors, etc. In some embodiments, monitoring element 188 initiates the transfer of information from file transfer agent 198.

[00181] Figure 11 illustrates an example embodiment of gateway function 158 (which is functionally equivalent to gateway function 172). End-user device 100 (e.g., using service processor 115) establishes a connection with optional gateway proxy server 136 through firewall 132 and optional load balancer 134. In some embodiments, optional gateway proxy server 136 includes an access control list used to allow access to one or

IPR2025-01572
Apple EX1002 Page 69

more destination IP addresses only from IP addresses in the access control list (e.g., the list specifies IP addresses that may pass through), or to deny access from all IP addresses in the access control list and allow access from all other IP addresses (e.g., the list specifies IP addresses that will be blocked). Gateway proxy server 136 establishes a connection to gateway application server 138 through firewall 110.

[00182] In the embodiment shown in Figure 11, end-user device 100 can receive a variety of information from gateway application server 138. For example, end-user device can receive information or instructions based on entries by portal user 102 (e.g., available service plans, how to present the available service plans on a user interface, service plan classifications (e.g., user-paid, sponsored, etc.), promotional messages, service offers, notification messages, etc.). As another example, end-user device 100 can receive information in response to a request from end-user device 100 (e.g., a request for an account balance, a request for a record of purchase history, etc.). As another example, end-user device 100 can receive administrative content, such as, for example, software updates.

[00183] In some embodiments, gateway application server 138 determines when to send information to end-user device 100. In some embodiments, gateway application server 138 sends information to end-user device 100 after completing an authentication protocol. In some embodiments, gateway application server 138 sends information to end-user device 100 in response to request or activity by another element or function in the service controller (e.g., EAI server 128, portal application server 112, fraud server 129, reconciliation server 131, or credentialing application server 146). In some embodiments, gateway application server 138 sends information to end-user device 100 in response to a communication from end-user device 100. In some embodiments, the communication from end-user device 100 is a message in an authentication protocol. In some embodiments, gateway application server 138 sends information to end-user device 100 over a secure communication link.

[00184] As illustrated in Figure 11, end-user device 100 can also send information to gateway application server 138. For example, end-user device 100 may send reports

IPR2025-01572
Apple EX1002 Page 70

containing measures of or costs associated with end-user device 100's access network usage, user acknowledgments or responses to notification messages, device-detected fraud events, authentication messages, heartbeats (e.g., communications sent at regular intervals to provide information about the status of end-user device 100, such as, for example, to indicate that end-user device 100 is functioning properly), or requests (e.g., to purchase a service plan, to retrieve a purchase history, to check an account balance, etc.). As will now be understood by a person having ordinary skill in the art in view of the disclosures herein, the communication link between end-user device 100 and gateway application server 138 can be used to support a wide variety of information exchanges between end-user device 100 and the service controller.

[00185] As illustrated in Figure 11, gateway application server 138 is also capable of receiving information through message bus 130. In some embodiments, gateway application server 138 passes messages only within the same security zone. In some embodiments, gateway application server 138 receives information through message bus 130 from portal user 102 or from EAI server 128. As mentioned previously, message bus 130 may be any inter-process communication mechanism and may be different between different pairs of elements. In some embodiments, message bus 130 provides web services connectivity between EAI server 128 and gateway application server 138, and EAI server 128 uses web services to send information to gateway application server 138. In some embodiments, the web services calls occur only within the same security zone.

[00186] Gateway application server 138 retrieves information from and stores information in database cluster 116, communicating through firewall 114. In some embodiments, gateway application server 138 stores information from end-user device 100 in database cluster 116. In some embodiments, gateway application server 138 retrieves queued messages destined for end-user device 100 from database cluster 116. For example, gateway application server 138 may retrieve from database 116 and send to end-user device one or more of the following types of information: control, charging, or notification policies; promotional messages; service plan updates; end-user device configuration updates (e.g., related to the look and feel of a user interface on end-user device 100, etc.); a link to a software download.

IPR2025-01572
Apple EX1002 Page 71

[00187] In some embodiments, gateway application server 138 receives an authentication request from end-user device 100 and, based on the authentication request, retrieves a stored credential from database cluster 116 to assist in authenticating end-user device 100. In some embodiments, the authentication request from end-user device 100 comprises a credential associated with end-user device 100 or associated with a subscriber. In some embodiments, the credential is associated with a device identifier, or a subscriber identifier, or both a device identifier and a subscriber identifier. In some embodiments, the credential is one or more of a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. In some embodiments, gateway application server 138 determines, based on the received credential and the stored credential, whether to proceed with communications with end-user device 100. In some embodiments, gateway application server 138 determines whether the credential sent by end-user device 100 is valid. In some embodiments, gateway application server 138 checks whether the credential sent by end-user device 100 has been revoked. In some embodiments, gateway application 138 determines whether the credential sent by end-user device 100 appears on a revocation list. In some embodiments, if the credential is a certificate, gateway application server 138 checks whether the certificate is on a certificate revocation list, where the certificate revocation list may be stored within or external to service controller 122 (e.g., in database cluster 116, in credentialing application server 146, in a separate certificate revocation list server, etc.).

[00188] In some embodiments, if the credential sent by end-user device 100 is valid, gateway application server 138 communicates with end-user device 100 using the credential for the purpose of exchanging service-related information or software. In some embodiments, the communication using the credential is over a secure communication link. In some embodiments, the secure communication link uses the SSL protocol. In some embodiments, the service-related information comprises a plan catalog. In some embodiments, the service-related information comprises a control, charging, or notification policy. In some embodiments, the service-related information comprises a promotional message or advertisement. In some embodiments, the service-related information comprises a usage measure or a cost measure. In some embodiments,

IPR2025-01572
Apple EX1002 Page 72

the service-related information comprises an account balance. In some embodiments, the service-related information comprises a fraud alert. In some embodiments, the service-related information comprises a request from end-user device 100. In some embodiments, the service-related information comprises a response to a request from end-user device 100. In some embodiments, the service-related information comprises a request to end-user device 100. In some embodiments, the service-related information comprises a response to a request to end-user device 100. In some embodiments, the service-related information is configured to cause end-user device 100 to take a specific action. In some embodiments, the specific action is to be taken immediately. In other embodiments, the specific action is to be scheduled. In some embodiments, the specific action is to block, allow, rate-limit, or delay access to the access network by end-user device 100.

[00189] Figure 11 shows three agents that communicate with monitoring element 188. As illustrated in Figure 11, gateway proxy server 136 includes notification agent 200, which communicates through firewall 186 with monitoring element 188, and gateway application server 138 includes notification agent 202 and log forwarder 204, both of which also communicate with monitoring element 188 through firewall 186.

[00190] Notification agent 200 and notification agent 202 provide information to monitoring element 188. In some embodiments, one or both of notification agents 200 and 202 are SNMP agents. In some embodiments, the information provided by one or both of notification agents 200 and 202 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by one or both of notification agents 200 and 202 is in response to a request from monitoring element 188.

[00191] In some embodiments, monitoring element 188 responds to information sent by notification agent 200 or 202. For example, in some embodiments, monitoring element 188 sends notification agent 200 or 202 a message directing (respectively) gateway proxy server 136 or gateway application server 138 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to

IPR2025-01572
Apple EX1002 Page 73

determine whether a connected system is functional, etc.). In some embodiments, monitoring element 188 directs gateway proxy server 136 to test the communication path to gateway application server 138.

[00192] Log forwarder 204 also sends information to monitoring element 188. In some embodiments, log forwarder 204 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, gateway application server 138 generates log files, and log forwarder 204 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 204 sends a system log, an information log, a debug log, an error log, information about a fatal event, etc. In some embodiments, gateway application server 138 initiates the transfer of information from log forwarder 204 to monitoring element 188.

[00193] Figure 12 illustrates an example embodiment of credentialing function 157 (which is functionally equivalent to credentialing function 173 shown in Figure 8). End-user device 100 communicates with optional credentialing proxy server 144 through firewall 140 and optional load balancer 142. In some embodiments, end-user device 100 establishes a secure connection over the Internet to communicate with credentialing proxy server 144. Credentialing proxy server 144 communicates through firewall 110 with credentialing application server 146. Credentialing application server 146 retrieves information from and stores information in database cluster 116, communicating through firewall 114.

[00194] As described herein, the credentialing function enhances the security of DAS systems. In some embodiments, credentialing application server 146 receives a request from end-user device 100 (e.g., using service processor 115) for a credential. In some embodiments, the credential request from end-user device 100 to credentialing application server 146 includes a device identifier (e.g., any identifier associated with the end-user device) and a subscriber identifier (e.g., any identifier associated with the subscriber who uses or authorizes the use of the end-user device). In some embodiments,

IPR2025-01572
Apple EX1002 Page 74

the credential request comprises a hash of a device identifier and a subscriber identifier. In some embodiments, the hash is salted. In some embodiments, credentialing application server 146 generates a credential based on the credential request from end-user device 100, stores the credential in database cluster 116, and sends the credential to end-user device 100. In some embodiments, credentialing application server 146 stores the device identifier and the new credential separately in database cluster 116. In some embodiments, credentialing application server 146 stores the device identifier and new credential as a single entry comprising their combination (e.g., a hash). In some embodiments, end-user device 100 stores the credential in local memory and thereafter uses the credential for secure communications with the service controller (e.g., with gateway application server 138).

[00195] Figure 12 shows three agents that communicate with monitoring element 188. As illustrated in Figure 12, credentialing proxy server 144 includes notification agent 210, which communicates through firewall 186 with monitoring element 188, and credentialing application server 146 includes notification agent 212 and log forwarder 214, both of which also communicate with monitoring element 188 through firewall 186.

[00196] Notification agent 210 and notification agent 212 provide information to monitoring element 188. In some embodiments, one or both of notification agents 210 and 212 are SNMP agents. In some embodiments, the information provided by one or both of notification agents 210 and 212 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by one or both of notification agents 210 and 212 is in response to a request from monitoring element 188.

[00197] In some embodiments, monitoring element 188 responds to information sent by notification agent 210 and 212. For example, in some embodiments, monitoring element 188 sends notification agent 210 and 212 a message directing (respectively) credentialing proxy server 144 or credentialing application server 146 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to determine whether a connected system is functional, etc.). In some

IPR2025-01572
Apple EX1002 Page 75

embodiments, monitoring element 188 directs credentialing proxy server 144 to test the communication path to credentialing application server 146.

[00198] Log forwarder 214 also sends information to monitoring element 188. In some embodiments, log forwarder 214 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, credentialing application server 146 generates log files, and log forwarder 214 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 214 sends a system log, an information log, a debug log, an error log, information about a fatal event, etc. In some embodiments, credentialing application server 146 initiates the transfer of information from log forwarder 214 to monitoring element 188.

[00199] Figure 13 illustrates an example embodiment of EAI server 128 when it supports the communication paths shown in Figures 1A, 1B, and 1C. As illustrated in Figure 13, EAI server 128 retrieves carrier file 118 from file server 126 and places output file 120 on file server 126. In some embodiments, EAI server 128 initiates the transfer of carrier file 118 from file server 126 and the transfer of output file 120 to file server 126. As shown in Figure 13, transfers of information between EAI server 128 and file server 126 are through firewall 110. As shown in Figure 13, there is no message queue to allow file server 126 to inform EAI server 128 that there is a file available for EAI server 128.

[00200] Figure 13 also illustrates one embodiment of a communication path between EAI server 128 and gateway application server 138. Information flows directly from EAI server 128 to gateway application server 138. Information from gateway application server 138 to EAI server 128 flows through message bus 130.

[00201] EAI server 128 also communicates directly with portal application server 122 through web services interface 226. EAI server 128 communicates with carrier IT/billing 139 using EAI interface 231, with information passing through firewall 235.

[00202] EAI server 128 communicates through firewall 114 with database cluster

IPR2025-01572
Apple EX1002 Page 76

116. In some embodiments, EAI server 128 retrieves service-related information from database cluster 116 (e.g., information entered by or derived from information entered by portal user 102) and provides the information to gateway application server 138 for sending to end-user device 100.

[00203] Figure 13 shows that EAI server 128 includes two agents that communicate with monitoring element 188 through firewall 186. Notification agent 228 provides information to monitoring element 188. In some embodiments, notification agent 228 is an SNMP agent. In some embodiments, the information provided by notification agent 228 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by notification agent 228 is in response to a request from monitoring element 188.

[00204] In some embodiments, monitoring element 188 responds to information sent by notification agent 228. For example, in some embodiments, monitoring element 188 sends notification agent 228 a message directing EAI server 128 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to determine whether a connected system is functional, etc.).

[00205] Log forwarder 230 also sends information to monitoring element 188. In some embodiments, log forwarder 230 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, EAI server 128 generates log files, and log forwarder 230 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 230 sends a system log, an information log, a debug log, an error log, information about a fatal event, etc. In some embodiments, EAI server 128 initiates the transfer of information from log forwarder 230 to monitoring element 188.

[00206] Figure 14 illustrates an example embodiment that is similar to the embodiment shown in Figure 13. In Figure 14, file server 126 accesses message bus 130 through firewall 110. In some embodiments, file server 126 places information for EAI server 128 on message bus 130. The embodiment of Figure 14 allows file server 126 to

IPR2025-01572
Apple EX1002 Page 77

notify EAI server 128 that there is a file available on file server 126, thus potentially reducing the time before EAI server 128 retrieves the file.

[00207] Figure 15 illustrates an example embodiment with an alternate mechanism to allow file server 126 to notify EAI server that there is a file available on file server 126. In the embodiment of Figure 15, EAI server 128 includes dedicated message bus 233, and file server 126 places information on message bus 233, communicating through firewall 110. EAI server 128 consumes message bus 233 and then initiates a procedure to retrieve the file from file server 126.

[00208] Figure 16 illustrates an example embodiment that is similar to the embodiment of Figure 13, except that EAI server 128 communicates with carrier IT/billing element 139 through external EAI interface 238, which it reaches through firewall 235. As would be understood by a person of ordinary skill in the art in view of the disclosures herein, external EAI interface 238 may be used in the embodiments of Figures 7A, 7B, and 7C, as well.

[00209] Figure 17 illustrates an example embodiment of fraud server 129. As illustrated in Figure 17, fraud server 129 communicates with EAI server 128 through message bus 130. EAI server 128 communicates with carrier IT/billing element 139 through firewall 235, external EAI interface 238, and firewall 237. Although EAI interface 238 is illustrated as external to EAI server 128, one of ordinary skill in the art will understand in light of the disclosures herein that the EAI interface may be part of EAI server 128, and, in such a case, either firewall 235 or firewall 237 may be eliminated. Fraud server 129 retrieves information from and stores information on database cluster 116 through firewall 114. In some embodiments, fraud server 129 stores fraud events on database cluster 116. In some embodiments, fraud server 129 retrieves information to meet a request from EAI server 128 or gateway application server 138 (e.g., carrier data usage records, device-assisted usage records, etc.). In some embodiments, fraud server 129 places a message on message bus 130 to tell EAI server 128 that fraud server 129 has completed a task.

[00210] As illustrated in Figure 17, fraud server 129 includes notification agent

IPR2025-01572
Apple EX1002 Page 78

234 and log forwarder 236. Notification agent 234 provides information to monitoring element 188. In some embodiments, notification agent 234 is an SNMP agent. In some embodiments, the information provided by notification agent 234 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by notification agent 234 is in response to a request from monitoring element 188.

[00211] In some embodiments, monitoring element 188 responds to information sent by notification agent 234. For example, in some embodiments, monitoring element 188 sends notification agent 234 a message directing fraud server 129 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to determine whether a connected system is functional, etc.).

[00212] Log forwarder 236 also sends information to monitoring element 188. In some embodiments, log forwarder 236 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, fraud server 129 generates log files, and log forwarder 236 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 236 sends a system log, an information log, a debug log, an error log, information about a fatal event, etc. In some embodiments, fraud server 129 initiates the transfer of information from log forwarder 236 to monitoring element 188.

[00213] Figure 18 illustrates an example embodiment of reconciliation server 131. As illustrated in Figure 18, reconciliation server 131 communicates with EAI server 128 through message bus 130. EAI server 128 communicates with carrier IT/billing element 139 through firewall 235, external EAI interface 238, and firewall 237. Although EAI interface 238 is illustrated as external to EAI server 128, one of ordinary skill in the art will understand in light of the disclosures herein that the EAI interface may be part of EAI server 128, and, in such a case, either firewall 235 or firewall 237 may be eliminated. EAI server 128 also communicates with file server 126 through firewall 110, as described in the context of Figures 7A through 7D. Reconciliation server 131 retrieves

IPR2025-01572
Apple EX1002 Page 79

information from and stores information on database cluster 116 through firewall 114. In some embodiments, reconciliation server 131 stores outbound usage records to be sent to the carrier on database cluster 116. In some embodiments, the outbound usage records comprise device-assisted measures of access network usage by an end-user device, such as end-user device 100. In some embodiments, reconciliation server 131 places a message on message bus 130 to tell EAI server 128 or file server 126 that reconciliation server 131 has completed a task. In some embodiments, reconciliation server 131 retrieves information from database cluster 116 to meet a request from EAI server 128 or gateway application server 138 (e.g., carrier data usage records, device-assisted usage records, etc.).

[00214] As illustrated in Figure 18, reconciliation server 131 includes notification agent 238 and log forwarder 240. Notification agent 238 provides information to monitoring element 188. In some embodiments, notification agent 238 is an SNMP agent. In some embodiments, the information provided by notification agent 238 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by notification agent 238 is in response to a request from monitoring element 188.

[00215] In some embodiments, monitoring element 188 responds to information sent by notification agent 238. For example, in some embodiments, monitoring element 188 sends notification agent 238 a message directing reconciliation server 131 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to determine whether a connected system is functional, etc.).

[00216] Log forwarder 240 also sends information to monitoring element 188. In some embodiments, log forwarder 240 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, reconciliation server 131 generates log files, and log forwarder 240 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 240 sends a system log, an information log, a debug log, an error log,

IPR2025-01572
Apple EX1002 Page 80

information about a fatal event, etc. In some embodiments, reconciliation server 131 initiates the transfer of information from log forwarder 240 to monitoring element 188.

[00217] Figure 19 illustrates an example embodiment of message bus 130 as depicted in Figures 1A through 1C. EAI server 128 both places information on and retrieves information from message bus 130 through message queue 242. Gateway application server 138 places information on message bus through message queue 242. As needed to manage the message bus, message queue 242 moves entries in message queue 242 to or from master/slave message queue storage 248.

[00218] As illustrated in Figure 19, message bus 130 includes notification agent 244 and log forwarder 246. Notification agent 244 provides information to monitoring element 188. In some embodiments, notification agent 244 is an SNMP agent. In some embodiments, the information provided by notification agent 244 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by notification agent 244 is in response to a request from monitoring element 188.

[00219] In some embodiments, monitoring element 188 responds to information sent by notification agent 244. For example, in some embodiments, monitoring element 188 sends notification agent 244 a message directing message bus 130 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to determine whether a connected system is functional, etc.).

[00220] Log forwarder 246 also sends information to monitoring element 188. In some embodiments, log forwarder 246 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, message bus 130 generates log files, and log forwarder 246 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 246 sends a system log, an information log, a debug log, an error log, information about a fatal event, etc. In some embodiments, message bus 130 initiates the transfer of information from log forwarder 246 to monitoring element 188.

Figure 20 illustrates an example embodiment incorporating two data centers, data center 242 and data center 250, to assist in providing geo-redundancy in the network. Data centers 242 and 250 are functionally equivalent but physically distinct. Database node 260 illustrates the functionalities that are also present in database node 254. Database node 260 is part of database cluster 116, and database node 254 is part of database cluster 174 (both shown in Figure 8). Database node 260 includes cluster service 262, which is responsible for managing the cluster of database nodes (e.g., verifying the node operating environment, verifying consistency of data stored in storage 264, performing failover to secondary database node, receiving and processing messages from listener 270, etc.), and storage 264, which is the database used for storing all of the data provided by portal application server 112, gateway application server 138, EAI server 128, fraud server 129, reconciliation server 131, credentialing application server 146, etc., for persistence and retrieval at a later time. Database node 260 also includes listener 270, which detects database access requests made by portal application server 112, EAI server 128, fraud server 129, reconciliation server 131, gateway application server 138, and credentialing application server 146 through firewall 114.

[00221] As illustrated in Figure 20, database node 260 also includes notification agent 266 and log forwarder 268, which communicate with monitoring element 188 through firewall 186. Notification agent 266 provides information to monitoring element 188. In some embodiments, notification agent 266 is an SNMP agent. In some embodiments, the information provided by notification agent 266 includes unsolicited notifications of events (e.g., disk full, memory error, SNMP traps, etc.). In some embodiments, information provided by notification agent 266 is in response to a request from monitoring element 188.

[00222] In some embodiments, monitoring element 188 responds to information sent by notification agent 266. For example, in some embodiments, monitoring element 188 sends notification agent 266 a message directing database node 260 to perform an action (e.g., run a program, run a test query to validate that the system is functional, run a program to determine whether a connected system is functional, etc.).

IPR2025-01572
Apple EX1002 Page 82

[00223] Log forwarder 268 also sends information to monitoring element 188. In some embodiments, log forwarder 268 sends information configured to assist in diagnosing problems with a system or service controller application. For example, in some embodiments, database node 260 generates log files, and log forwarder 268 sends the log files to monitoring element 188. In some embodiments, the log files are generated for individual service controller applications. In some embodiments, log forwarder 268 sends a system log, an information log, a debug log, an error log, information about a fatal event, etc. In some embodiments, database node 260 initiates the transfer of information from log forwarder 268 to monitoring element 188.

Secure Service Processor Operating Environments

[00224] In some embodiments, it is advantageous to store or implement certain portions or all of service processor 115 (e.g., agents, etc.) 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 placed in a secure area of the operating system (e.g., in a kernel) so that it cannot be removed or, if it is removed, it must be replaced for proper device operation to resume. 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 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 shown in Figure 2. 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.

[00225] Agent communication bus 1630 represents a functional description for providing communication for the various service processor 115 agents and functions. In

IPR2025-01572
Apple EX1002 Page 83

some embodiments, such as the embodiment shown in Figure 2, the architecture of agent communication bus 1630 is generally multipoint-to-multipoint so that any agent can communicate with any other agent, service controller 122, or in some cases other components of end-user device 100, such as user interface 1697 and/or modem components. 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, agent communication bus 1630 is secured, signed, encrypted, hidden, partitioned and/or otherwise protected from unauthorized monitoring or usage.

[00226] In some embodiments, there are multiple layers of security applied to 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 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 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, service control device link 1691 is assumed to be equivalent to an agent for communication purposes, and, in the case of service control device link 1691, the communication is not restricted to agent communication bus 1630 but also extends to 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.

[00227] Various forms of message encryption and security framework techniques can be applied to encrypt and/or secure agent communication bus 1630, including one or

IPR2025-01572
Apple EX1002 Page 84

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; user interface (UI) messages are only analyzed and passed, in which user interface 1697 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 access control integrity agent 1694 or heartbeat function can become point to multipoint secure communications hubs.

[00228] In some embodiments, the design of agent communication bus 1630 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 agent communication bus 1630 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

IPR2025-01572
Apple EX1002 Page 85

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 agent communication bus 1630 to meet a particular set of product and desired functional requirements.

[00229] In some embodiments, service processor 115 includes a DDR processor located in a secure execution environment, and this DDR processor can be used advantageously to improve security of device-assisted services systems. Co-pending United States patent application number 13/247,998, entitled "Secured Device Data Records" and incorporated by reference herein, describes embodiments of a DDR processor. In some embodiments, the DDR processor sends a sequence of secure device data records (DDRs) to a network element (e.g., via a secure channel). In some embodiments, the DDR processor is configured with an access controller that restricts end-user device 100's network access to a predetermined set of network destinations or functions if any of the DDR processor, service processor 115, or service controller 122 detects an error or potential fraud in one or more reports in the sequence of secure DDRs.

Service Processor Enrollment

[00230] In some embodiments, before service processor 115 of end-user device 100 participates in device-assisted services, it enrolls with service controller 122. In the enrollment process, service controller 122 (using, e.g., credentialing application server 146, a network element such as authentication credential server 220, etc.) allocates a device credential to service processor 115. In some embodiments, the credential is one or more of a certificate, a key, a shared secret, a password, a hash, a shared algorithm, or any other item of information that allows service controller 122 to confirm the identity of service processor 115. After service controller 122 has allocated the device credential, service controller 122 can use the device credential when it needs to authenticate service processor 115, such as, for example, before end-user device 100 sends device-based usage reports to gateway application server 138.

[00231] Figure 21 illustrates a set of steps end-user device 100 takes to obtain a

IPR2025-01572
Apple EX1002 Page 86

credential from service controller 122 in accordance with some embodiments. At step 1000, end-user device 100 creates a key pair. At step 1002, end-user device 100 generates an identity credential using the key pair. In some embodiments, the identity credential comprises a device identifier and a subscriber identifier. At step 1004, using the identity credential generated in step 1002, end-user device 100 generates a request for the service controller credential. At step 1006, end-user device 100 sends the request for the service controller credential to the service controller. At step 1008, end-user device 100 receives a credential from service controller 122. In some embodiments, the service controller credential is a public key credential. At step 1010, end-user device 100 verifies the service controller credential signing chain. As will be appreciated by a person having ordinary skill in the art, the process of verifying the authenticity and validity of a newly received credential involves checking all of the credentials in the chain of credentials from the original, universally trusted certificate authority, through any intermediate certificate authorities, down to the credential just received, which may be referred to as the end credential. The end credential is trusted if each credential in that credential's chain is properly issued and valid.

[00232] If end-user device 100 successfully verifies the service controller credential signing chain in step 1010, at step 1012 end-user device 100 generates a credential signing request using the service controller credential received in step 1008. In some embodiments, the credential signing request comprises a subscriber identifier and a device identifier. At step 1014, end-user device 100 sends the credential signing request to the service controller. In some embodiments, the credential signing request comprises a challenge password. At step 1016, end-user device 100 receives a device credential from service controller 122. At step 1018, end-user device 100 stores the device credential in local memory. In some embodiments, service controller 122 (e.g., credentialing application server 146) comprises a simple certificate enrollment protocol (SCEP) server, and the credential is a certificate. In some embodiments, messages sent and received by end-user device 100 are encrypted. In some embodiments, the service controller credential and device credential are 2048-bit RSA public key credentials. In some embodiments, service controller 122 and end-user device 100 communicate using a

IPR2025-01572
Apple EX1002 Page 87

session key.

[00233] Figure 22 illustrates the steps service controller 122 (e.g., using credentialing application server 146) performs to provide a device credential to end-user device 100 in some embodiments. At step 1030, service controller 122 receives a request for a service controller credential from end-user device 100. In some embodiments, the request comprises a device identifier and a subscriber identifier. At step 1032, service controller 122 sends the service controller credential to end-user device 100. At step 1034, service controller 122 receives a credential signing request comprising a challenge password from end-user device 100. In some embodiments, the request comprises a device identifier and a subscriber identifier. At step 1036, service controller 122 verifies that the subscriber identifier is listed in database cluster 116. At optional step 1038, service controller 122 verifies the device identifier from a device table. In some embodiments, the device table resides in database cluster 116 and contains a list of valid devices that are allowed to connect to service controller 122. At step 1040, service controller 122 validates the challenge password using the device identifier. At step 1042, service controller 122 stores the device identifier in database cluster 116 as associated with the subscriber identifier associated with end-user device 100. At step 1044, service controller 122 generates a device credential for end-user device 100 by obtaining a primary key from database cluster 116. At step 1046, service controller 122 stores the device credential in database cluster 116 as associated with the subscriber identifier and the device identifier associated with end-user device 100. At step 1048, service controller 122 sends the device credential to end-user device 100. In some embodiments, service controller 122 (e.g., using credentialing application server 146) comprises a simple certificate enrollment protocol (SCEP) server, and the credential is a certificate. In some embodiments, messages sent and received by service controller 122 are encrypted. In some embodiments, the service controller credential and device credential are 2048-bit RSA public key credentials. In some embodiments, service controller 122 and end-user device 100 communicate using a session key.

[00234] Although the steps are presented in Figures 6B and 6C in a particular order, as will be appreciated by a person having ordinary skill in the art in light of the

IPR2025-01572
Apple EX1002 Page 88

disclosures herein, the ordering of some steps can be modified. As simple examples, steps 1010 and 1012 of Figure 21 can be interchanged, and in Figure 22, step 1048 can be performed before 1046, step 1038 can be performed before step 1036, etc.

[00235] In some embodiments, service controller 122 is configured to allocate multiple credentials to different end-user devices associated with a single subscriber identifier. Figure 23 illustrates an example of such an embodiment. As shown in Figure 23, at step 1050, service controller 122 (e.g., using credentialing application server 146) receives an authentication request comprising a device identifier and a subscriber identifier from end-user device 100. At step 1052, service controller 122 verifies that the subscriber identifier is listed in database cluster 116. If the subscriber identifier is listed in database cluster 116, at step 1054, service controller 122 verifies that the device identifier sent by end-user device 100 is not already in database cluster 116. If the device identifier sent by end-user device 100 is not already in database cluster 116, at step 1056, service controller 122 obtains (e.g., by generating or allocating) a new credential for end-user device 100. At step 1058, service controller 122 stores both the device identifier and the new credential in database 116 as associated with the subscriber identifier. In some embodiments, the device identifier and the new credential are stored in separate fields of database cluster 116. In some embodiments, the device identifier and new credential are stored as a single entry comprising their combination (e.g., a hash). In some embodiments, service controller 122 monitors or tracks end-user device enrollment attempts. In some embodiments, credentialing application server 146 or another element of the service controller (e.g., a fraud element such as fraud server 129) notifies the carrier about credentialing enrollment attempts, successful enrollments, or unsuccessful enrollments.

Service Processor Authentication; Starting and Stopping a Data Session

[00236] To achieve an overall network service policy, the network portion of the access network service policy may be configured to work in conjunction with the device-based portion of the access network service policy to achieve an overall combined network service policy. If the device agents required to implement the device portion of the access network service policy are not present on the device or are not properly

IPR2025-01572
Apple EX1002 Page 89

configured because of tampering or other undesirable activities, then the overall combined network service policy can be in error or may not be possible to achieve, potentially resulting in an undesired network service policy implementation. In such cases, it is desirable for a network system to be employed to detect this condition and modify the network portion of an access network service policy enforced by the network-based elements so that a desired network service policy enforcement may be achieved.

[00237] Examples of when it may be advantageous to adapt the network portion of an access network service policy in order to account for a missing or improperly configured service processor include but are not limited to: (i) a device credential has been moved to a device that does not have a service processor, (ii) a device credential has been moved to a device with a service processor with a different configuration than the service processor originally associated with the device credential, (iii) a device service processor has been tampered with or has an improper configuration.

[00238] In some embodiments, service controller 122 detects the presence and proper configuration of a service processor, or lack thereof, in the end-user device. If the service processor is present and properly configured, service controller 122 causes a first network portion of an access network service policy to be enforced in the network, the first network portion of an access network service policy being configured to provide counterpart policy enforcement to a device portion of an access network service policy to achieve a first desired overall access network service policy. If, on the other hand, the service processor is not both present and properly configured, service controller 122 causes a second network portion of an access network service policy to be enforced in the network, wherein the second network portion of the access network service policy is configured to operate without a device counterpart policy to achieve a second desired overall access network service policy.

[00239] In some embodiments, a trusted service policy implementation comprises service controller 122 authenticating and authorizing service processor 115. In some embodiments, the authentication comprises receiving and confirming a service processor certificate. In some embodiments, the authentication comprises receiving and confirming

IPR2025-01572
Apple EX1002 Page 90

a service processor certificate that is based on a shared secret between service processor 115 and service controller 122. In some embodiments, the shared secret is unique for a given service processor 115.

[00240] In some embodiments, the process to establish a trusted service policy implementation comprises service processor 115 sharing two or more types of credentials with service controller 118, wherein the credentials include two or more of a service processor credential, a device credential, and a user or subscriber credential. In some embodiments, a portion of the process to establish a trusted service policy implementation includes end-user device 100 (e.g., service processor 115) sharing a service processor credential, a device credential, and a user or subscriber credential with service controller 122.

[00241] In some embodiments, establishing a trusted service policy implementation comprises service controller 122 receiving a certificate or hash result from a service processor element or agent acting on a portion of service processor 115 (for example, access control integrity agent 1694 performing a hash or certificate check on another service processor agent).

[00242] Figure 24 illustrates an example embodiment of a process to start or stop a data session with SGSN notification. End-user device 100 attempts to start a data session by sending a "GPRS Attach" message to SGSN 2230. SGSN 2230 notifies service controller 122 that end-user device 100 has started a data session. Service controller 122 waits for a pre-determined time, for example, one minute, to receive a login or authentication request from service processor 115. In some embodiments, service controller 122 sets a login timer. If service controller 122 receives the login or authentication request before the timer expires, it attempts to authenticate service processor 115.

[00243] One or more authentication errors may occur when service controller 122 attempts to authenticate service processor 115. For example, service processor 115 may have invalid credentials. As another example, service processor 115 may send invalid application or kernel signatures. As another example, service processor 115 may report

IPR2025-01572
Apple EX1002 Page 91

end-user device "root" detection errors. As another example, service processor 115 may contact service controller 122 using an identifier that is already in use by a different end-user device.

[00244] If service controller 122 does not receive the request from service processor 115 within the pre-determined time, or if service controller 122 is unable to authenticate service processor 115 for some reason, service controller 122 assumes that either (1) end-user device 100 does not contain a service processor, and is therefore unable to participate in device-assisted services, or (2) although end-user device 100 has a service processor, service processor 115 has been disabled. Service controller 122 sends a notification ("No active SP" message) to data rating element 2220 to indicate that end-user device 100 does not have the ability to provide the information necessary for data mediation element 2210 to generate detailed data usage reports (referred to herein as "micro-CDRs"). In some embodiments, service controller 122 sends a trigger to data mediation element 2210 to indicate that end-user device 100 should be charged for usage at "standard" bulk rates. In some embodiments, service controller 122 specifies a "standard" bulk rate charging code in the charging data records (CDRs) it sends to data mediation element 2210. In some embodiments, data rating element 2220 determines data usage by end-user device 100 based on carrier-based records (e.g., records of end-user device 100's usage of data over access network 10).

[00245] If service controller 122 receives the login or authentication request from service processor 115 within the pre-determined time and successfully authenticates service processor 115, service controller 122 sends a notification ("Device OK" message) to data rating element 2220 to indicate that end-user device 100 has a service processor and is capable of supporting device-assisted services. In some embodiments, data rating element 2220 expects to receive "micro-CDR" reports from data mediation element 2210 when service controller 122 has determined that end-user device 100 has an active service processor. In some embodiments, data rating element 2220 determines usage based on the micro-CDRs, which contain more granular information than ordinary CDRs. For example, whereas an ordinary CDR might simply report that an end-user device used 100 Megabytes (MB) of data, a set of micro-CDRs might report that the end-user device

IPR2025-01572
Apple EX1002 Page 92

used 15 MB of e-mail, 35 MB of social networking, and 50 MB of streaming video.

[00246] In some embodiments, data mediation element 2210 sends carrier-based usage reports (e.g., CDRs) to service controller 122. Service controller 122 queries usage database 2200 for device-based usage reports (e.g., micro-CDRs) for end-user device 100. Service controller 122 determines the data usage of end-user device 100 from the carrier-based usage reports. Service controller 122 also determines the data usage of end-user device 100 from the device-based usage reports. In some embodiments, described in more detail below, service controller 122 compares the usage determined from the carrier-based usage reports to the usage determined from the device-based usage reports. If service controller 122 determines that the two usage measures do not match (e.g., are not identical or are not within a threshold of each other), service controller 122 sends a notification (e.g., a fraud alert) to data rating element 2220 to indicate that the end-user device is in a potential fraud state, and data rating element 2220 should bill usage for end-user device 100 based on carrier-based usage reports. Service controller 122 sends the carrier-based usage reports and device-based usage reports to data mediation element 2210.

[00247] When the "GPRS detach" message is received by SGSN 2230, SGSN 2230 sends a notification to service controller 122 that the data session for end-user device 100 is closed.

[00248] Figure 25 illustrates an example embodiment of a process to start or stop a data session with GGSN notification. The process is similar to that described with reference to Figure 24, except in how the data session starts and ends. End-user device 100 starts a data session by sending data traffic to GGSN 2240. GGSN 2240 recognizes the start of a new data session and notifies service controller 122 that end-user device 100 has started a data session. When GGSN 2240 determines that the data session has closed, it sends a notification to service controller 122 that the data session for end-user device 100 is closed.

[00249] Figure 26 illustrates an example embodiment of a process to start or stop a data session when a AAA or RADIUS server (e.g., access network AAA server 1621)

IPR2025-01572
Apple EX1002 Page 93

provides start/stop accounting in a GSM/GPRS core data network. The process is similar to that described with reference to Figure 24, except that AAA or RADIUS 2242 authorizes the start of a new data session and notifies service controller 122 that end-user device 100 has started a data session. When AAA or RADIUS 2242 determines that the data session has closed, it sends a notification to service controller 122 that the data session is closed.

[00250] Figure 27 illustrates an example embodiment of a process to start or stop a data session when an OCS provides start/stop accounting in a GSM/GPRS core data network. The process is similar to that described with reference to Figure 24, except that after GGSN 2240 recognizes the start of a new data session with end-user device 100, GGSN 2240 queries OCS 2246 for a data lease. OCS 2246 authorizes the data session by returning a value representing an amount of data to GGSN 2240 (e.g., OCS 2246 sends a value of X bytes to GGSN 2240). OCS 2246 uses API 2244 to notify service controller 122 that end-user device 100 has started a data session. When GGSN 2240 determines that the data session has closed, it sends a notification to OCS 2246 indicating the amount of data left in the amount of data authorized by OCS 2246. OCS 2246 uses API 2244 to notify service controller 122 that the data session is closed.

[00251] Service processor 115 may successfully authenticate with service controller 122 but then subsequently send one or more fraud notifications. Examples of device fraud notifications that service processor 115 might send are: invalid service processor kernel signature, invalid service processor framework signature, invalid service processor application signature, service processor application unable to connect to service processor kernel, service processor application not receiving heartbeat messages from service processor kernel, service processor kernel missing, service processor framework missing, service processor application missing, hosts file tampered with or missing, service processor to service controller encryption failure, or device "root" detected. In some embodiments, in response to receiving a device fraud notification from service processor 115, service controller 122 generates a fraud alert.

End-User Device Kernel/Software Component Verification

IPR2025-01572
Apple EX1002 Page 94

[00252] In some embodiments, establishing a trusted service policy implementation comprises two service processor 115 elements performing a mutual authentication of one another and then acting on an error result if one occurs. Figure 28 illustrates an example embodiment of a procedure that a verifying software component on end-user device 100 may perform to verify the integrity of another software component on end-user device 100. Each of the software components can be, for example, a kernel, a library, an executable file, one or more interpreted, machine-readable instructions, a script, a service processor, or any other software component.

[00253] At step 1100, a verifying software component obtains the public key of a to-be-verified software component. At step 1102, the verifying software component generates a random number. At step 1104, the verifying software component generates an encrypted challenge using the random number and the to-be-verified software component's public key. At step 1106, the verifying software component sends the encrypted challenge to the to-be-verified software component. At step 1108, the verifying software component obtains an encrypted response from the to-be-verified software component. At step 1110, the verifying software component obtains its own private key. At step 1112, the verifying software component uses its own private key and the encrypted response to obtain a first decoded random number. At step 1114, the verifying software component verifies that the first decoded random number matches the generated random number. In some embodiments, if the first decoded random number does not match the generated random number, the verifying software component takes an action. In some embodiments, if the to-be-verified software component is an application, the action comprises restricting the application's ability to communicate over an access network. In some embodiments, the action comprises notifying a user of end-user device 100. In some embodiments, the action comprises notifying a network administrator. In some embodiments, if the to-be-verified software component is an application, the action is to apply a policy to attempted or successful communications associated with the application. In some embodiments, the action is to take a countermeasure, such as, for example, preventing a user from accessing the to-be-verified software component, preventing the to-be-verified software component from executing, or terminating the to-

IPR2025-01572
Apple EX1002 Page 95

be-verified software component (if it is running).

[00254] In some embodiments, if, in step 1114, the first decoded random number matches the generated random number, the verifying software component sends a message to service controller 122 (or another network element) indicating that the to-be-verified software component passed the test.

[00255] Figure 29 illustrates an example embodiment of a procedure that the to-be-verified software component can perform in response to the procedure of Figure 28. At step 1120, the to-be-verified software component obtains the encrypted challenge from the verifying software component. At step 1122, the to-be-verified software component obtains its own private key. At step 1124, the to-be-verified software component uses its own private key and the encrypted challenge to obtain a second decoded random number. At step 1126, the to-be-verified software component obtains the verifying component's public key. At step 1128, the to-be-verified software component uses the verifying component's public key and the second decoded random number to generate an encrypted challenge response. At step 1130, the to-be-verified component sends the encrypted challenge response to the verifying component.

End-User Device Application Authentication

[00256] In some embodiments, an installed software application on end-user device 100 cannot be modified, updated, or replaced unless the software purporting to be a modification, update, or replacement includes a credential that matches a credential associated with the installed application. In some embodiments, the installed-application credential is a name identifier. In some embodiments, the installed-application credential is a secure signature, certificate, or hash of the installed software application. In some embodiments, the installed-application credential is stored on end-user device 100. In some embodiments, the installed-application credential is accessible to service processor 115 (for example, via policy control agent 1692). In some embodiments, when an attempt is made to modify, update, or replace the installed software application, service processor 115 and/or a device operating system (OS) obtains both the installed-application credential and a credential associated with the purported modification, update,

IPR2025-01572
Apple EX1002 Page 96

or replacement. If the credential associated with the purported modification, update, or replacement matches the installed-application credential, service processor 115 allows the installed application to be modified, updated, or replaced.

[00257] Figure 30 illustrates a procedure to determine whether to allow a modification, update, or replacement of an installed software program. At step 1300, a component of end-user device 100 (e.g., service processor 115 or an operating system) obtains a credential associated with a software application installed on end-user device 100. At step 1302, a component of end-user device 100 (e.g., service processor 115 or an operating system) obtains a credential associated with software purporting to be a modification, update, or replacement of the installed software application. At step 1304, a component of end user-device 100 (e.g., service processor 115 or an operating system) determines whether the credential associated with the software purporting to be a modification, update, or replacement of the installed software application matches the credential associated with the installed software application. If there is a match, then at step 1306, a component of end-user device 100 (e.g., service processor 115 or an operating system) takes a first action. In some embodiments, the first action comprises allowing the software purporting to be a modification, update, or replacement of the installed application software to be installed on end-user device. In some embodiments, the first action further comprises notifying the service controller or a user of end-user device 100 of the modification, update, or replacement of the installed application software.

[00258] If, at step 1304, the credential associated with the software purporting to be a modification, update, or replacement of the installed software application does not match the credential associated with the installed software application, then at step 1308, a component of end-user device 100 (e.g., service processor 115 or an operating system) takes a fraud action. In some embodiments, the fraud action comprises restricting end-user device 100's access to an access network. In some embodiments, the fraud action comprises restricting an application's (e.g., the installed software application's) ability to communicate over an access network. In some embodiments, the fraud action comprises notifying a user of end-user device 100. In some embodiments, the fraud action

IPR2025-01572
Apple EX1002 Page 97

comprises notifying a network administrator or a network element of the credential mismatch. In some embodiments, the fraud action comprises applying a pre-determined billing rate for service usage by end-user device 100. In some embodiments, the fraud action comprises applying a pre-determined billing rate to service usage associated with the installed software application.

[00259] In some embodiments, end-user device 100 stores in memory (e.g., application program store 830 of Figure 38) an application program configured to execute on end-user device 100 to access one or more data services over an access network. The application program is associated with a credential that is also stored on end-user device 100 (e.g., in application program store 830, in application credential and policy store 810, etc.). End-user device 100 also stores (e.g., in application credential and policy store 810) a network access policy comprising one or more first instructions to be applied when the application program initiates or attempts to initiate communications over the first wireless access network. A device agent or a combination of device agents (e.g., application interface agent 1693, policy implementation agent 1690, modem selection and control 1811, etc.) determines when the application program initiates or attempts to initiate a communication over the access network (e.g., by monitoring end-user device 100 traffic flows, etc.) and applies the network access policy to the communication over the access network.

[00260] In some embodiments, end-user device 100 further comprises one or more device agents (e.g., service downloader 1663, access control integrity agent 1694, service monitor agent 1696, etc.) that detect when an entity (e.g., a user of end-user device 100, service controller 122, etc.) wishes or attempts to install update software on end-user device 100, where the update software purports to be a modification, update, or replacement of the application program. To improve security, the one or more device agents prevent modifications, updates, and replacements of the application software unless a credential associated with the purported update matches a credential of the installed application. For example, the one or more device agents obtain a credential associated with the application program that is already installed on end-user device 100, and a credential associated with a purported update to the installed application program.

IPR2025-01572
Apple EX1002 Page 98

If the one or more device agents determine that the credentials match, they allow the update software to be installed or to execute on end-user device 100.

[00261] In some embodiments, security of end-user device 100 is enhanced using agents on end-user device 100. In some embodiments, an agent on end-user device 100 (e.g., policy implementation agent 1690, policy control agent 1692, access control integrity agent 1694, or any other agent that can perform verification functions) determines if a hosts file is present on the end-user device and configured in an expected manner. If the hosts file is not present or is not configured in an expected manner, in some embodiments, the agent takes an action. In some embodiments, the action is to generate a fraud alert. In some embodiments, the action is to take a countermeasure, such as, for example, to block, delay, rate-limit, or quarantine access to the access network by end-user device 100. In some embodiments, the action is to provide a notification to a user of end-user device 100. In some embodiments, the action is to send a message to service controller 122.

[00262] In some embodiments, an agent on end-user device 100 (e.g., policy implementation agent 1690, policy control agent 1692, access control integrity agent 1694, or any other agent that can perform verification functions) determines if service processor 115 successfully completed the authentication procedure with service controller 122. In some embodiments, if the agent determines that service processor 115 has failed to complete the authentication procedure, the agent takes an action. In some embodiments, the action is to generate a fraud alert. In some embodiments, the action is to take a countermeasure, such as, for example, to block, delay, rate-limit, or quarantine access to the access network by end-user device 100. In some embodiments, the action is to provide a notification to a user of end-user device 100. In some embodiments, the action is to send a message to service controller 122.

[00263] In some embodiments, an agent on end-user device 100 (e.g., policy implementation agent 1690, policy control agent 1692, access control integrity agent 1694, or any other agent that can perform verification functions) determines whether the end-user device has been "rooted" or "jailbroken." As will be appreciated by a person

IPR2025-01572
Apple EX1002 Page 99

having ordinary skill in the art, rooting (or "jailbreaking") is a process that allows a user of a mobile device to attain privileged access (known as "root access") to the device's operating system, thereby potentially circumventing various limitations that might otherwise govern operation of the device. In some embodiments, if the agent determines that end-user device 100 has been rooted or jailbroken, the agent takes an action. In some embodiments, the action is to generate a fraud alert. In some embodiments, the action is to take a countermeasure, such as, for example, to block, delay, rate-limit, or quarantine access to the access network by end-user device 100. In some embodiments, the action is to provide a notification to a user of end-user device 100. In some embodiments, the action is to send a message to service controller 122.

[00264] In embodiments in which service processor 115 applies an access network policy that includes classification of attempted or successful service usage attributed to a device software application program, the identification of the software application program and association of the access network policy to the software application program comprises associating the access network policy with a known-application credential. In some embodiments, the credential is a name identifier. In some embodiments, the credential is a secure signature, certificate, or hash of the software application program. In some embodiments, the credential is stored on end-user device 100 by service processor 115 (for example, by policy control agent 1692), and service processor 115 and/or a device operating system (OS) obtains a run-time application credential for an application that intends to initiate execution and obtain access network service or has successfully initiated execution and obtained access network service usage. Policy control agent 1692 compares the run-time credential to the stored known-application credential, and if there is a credential match the access network policy associated with the known-application credential is applied to the application access network service usage.

[00265] In some embodiments, the known-application credential is stored on end-user device 100 and used for the comparison with the run-time application credential. In some embodiments, the run-time application credential is provided to an element of service controller 122 (for example, policy management server 1652) that in turn determines if it matches a known-application credential and, if so, the element of service

IPR2025-01572
Apple EX1002 Page 100

controller 122 provides the appropriate policy to service processor 115 (e.g., using gateway application server 138). In some embodiments, service processor 115 performs an application identity check on the run-time software program (for example, a secure hash, a secure hash based on a key provided by an element of service controller 122, or a signature check), and the result of this identity check is provided to the element of service controller 122, which in turn determines if it matches a known-application credential; if so, the element of service controller 122 provides the appropriate policy to service processor 115.

[00266] In some embodiments, if service processor 115 determines that a run-time application credential is intended, or may indicate an attempt, to spoof a known-application credential, a fraud action is taken. In some embodiments, if service controller 122 determines that a run-time application credential is intended, or may indicate an attempt, to spoof a known-application credential, a fraud action is taken. In some embodiments, the fraud action comprises restricting access to an access network for end-user device 100. In some embodiments, the fraud action comprises restricting an application's ability to communicate over an access network. In some embodiments, the fraud action comprises notifying a user of end-user device 100. In some embodiments, the fraud action comprises notifying a network administrator. In some embodiments, the fraud action comprises applying a pre-determined billing rate for service usage by end-user device 100. In some embodiments, the fraud action comprises applying a pre-determined billing rate for run-time application service usage by end-user device 100.

[00267] Figure 31 illustrates an example embodiment of a procedure that an end-user device, such as end-user device 100, can use to validate that an application installed on the end-user device is authentic. The application installed on the end-user device is associated with a credential that is stored in memory on the end-user device (e.g., application credential and policy store 810 of Figure 38). The credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1160, the end-user device obtains a known-valid credential associated with the application that is installed on the end-user device. The known-valid credential may be any type of credential, such as, for example, a certificate,

IPR2025-01572
Apple EX1002 Page 101

a key, a shared secret, a password, a hash, or a shared algorithm. In some embodiments, the end-user device obtains the known-valid credential from a trusted source. In some embodiments, the trusted source is the service controller. In some embodiments, the trusted source is a marketplace, an app store, an application author, a distributor, or a reseller. At step 1162, the end-user device determines whether the known-valid credential matches the credential of the installed application. If the credentials do not match, then in some embodiments the end-user device takes a first action at step 1164. In some embodiments, the first action is to generate a fraud alert. In some embodiments, the first action is to apply an unknown-application policy. In some embodiments, the first action is to notify a user of the end-user device. In some embodiments, the first action is to take a countermeasure, such as, for example, preventing a user from accessing the installed application, preventing the installed application from executing, or terminating the installed application (if it is running). In some embodiments, the first action is to send a notification to a network element.

[00268] If, in step 1162, the credentials match, the end-user device takes a second action at step 1166. In some embodiments, the second action is to apply a policy associated with the installed application. In some embodiments, the second action is to send a message to a server indicating that the end-user device is in a healthy state.

[00269] Figure 32 illustrates an example embodiment of a procedure that a service controller can use to validate that an application installed on an end-user device is authentic. At step 1170, the service controller obtains an application package from a trusted source. In some embodiments, the trusted source is a marketplace, an app store, an application author, a distributor, or a reseller. In some embodiments, the service controller obtains the application package in response to a request from the end-user device. At step 1172, the service controller extracts an application credential from the application package. The credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1174, the service controller sends the application credential to the end-user device. In some embodiments, the service controller later receives a status message from the end-user device after sending the application credential to the end-user device.

IPR2025-01572
Apple EX1002 Page 102

[00270] Figure 33 illustrates an example embodiment of another procedure that a service controller may use to validate that an application installed on an end-user device is authentic. At step 1180, the service controller receives a first application credential from the end-user device. The credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1182, the service controller obtains an application package from a trusted source. In some embodiments, the trusted source is a marketplace, an app store, an application author, a distributor, or a reseller. At step 1184, the service controller extracts a second application credential from the application package. At step 1186, the service controller determines whether the first application credential matches the second application credential. In some embodiments, if the credentials do not match, the service controller is configured to take an action (e.g., send a message to the end-user device, generate a fraud alert, send a message to the carrier, etc.).

[00271] Figure 34 illustrates an example embodiment of another procedure that an end-user device may use to validate that an application installed on the end-user device is authentic. At step 1190, the end-user device obtains a credential associated with an installed application. The credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1192, the end-user device generates a signed application credential using the installed-application credential and a device credential stored in local memory. The device credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1194, the end-user device sends the signed application credential to the service controller. At step 1196, the end-user device receives a message from the service controller regarding the authenticity of the installed application. In some embodiments, the message comprises, or is followed by a message with, instructions to take an action, such as, for example, to block the installed application from accessing the access network.

[00272] Figure 35 illustrates an example embodiment of another procedure that a service controller may use to validate that an application installed on an end-user device is authentic. At step 1200, the service controller receives a signed application credential

IPR2025-01572
Apple EX1002 Page 103

comprising an installed-application credential and a device credential from the end-user device. The device credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. In some embodiments, the signed application credential comprises a combination of the installed-application credential and the device credential (e.g., a hash). At step 1202, the service controller uses the device credential to process the signed application credential to obtain a first application credential. At step 1204, the service controller obtains a second application credential from a trusted source. In some embodiments, the service controller obtains an application package from the trusted source and extracts the second credential from the application package. In some embodiments, the trusted source is a marketplace, an app store, an application author, a distributor, or a reseller. At step 1206, the service controller determines whether the first application credential matches the second application credential. In some embodiments, if the first application credential does not match the second application credential, the service controller takes an action (e.g., sends a message to the end-user device, generates a fraud alert, sends a message to the carrier, etc.).

[00273] Figure 36 illustrates an example embodiment of another procedure that an end-user device may use to validate that an application installed on the end-user device is authentic. At step 1210, the end-user device receives a signed application credential from the service controller. The credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1212, the end-user device uses a device credential, stored in local memory, and the signed application credential to determine a first application credential. At step 1214, the end-user device obtains an installed-application credential that is associated with an application installed on the end-user device. The credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1216, the end-user device determines whether the first application credential matches the installed-application credential. In some embodiments, if the first application credential does not match the installed-application credential, the end-user device takes an action (e.g., sends a message to the service

IPR2025-01572
Apple EX1002 Page 104

controller, blocks the application from accessing the access network, executes instructions set by a control, charging, or notification policy, etc.). In some embodiments, the end-user device sends a message to the service controller to provide information about the authenticity of the application installed on the end-user device.

[00274] Figure 37 illustrates an example embodiment of another procedure that a service controller may use to validate that an application installed on an end-user device is authentic. At step 1220, the service controller obtains an application credential from a trusted source, wherein the application credential is associated with the installed application. The application credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. In some embodiments, the trusted source is a marketplace, an app store, an application author, a distributor, or a reseller. At step 1222, the service controller generates a signed application credential using the application credential and a device credential stored in local memory. In some embodiments, local memory is database cluster 116. In some embodiments, the device credential is a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step 1224, the service controller sends the signed application credential to the end-user device. In some embodiments, after sending the signed application credential to the end-user device, the service controller receives a message from the end-user device providing information about the authenticity of the application installed on the end-user device.

[00275] Figure 38 illustrates an example embodiment of end-user device 100 for implementing access network policy specific to a device application program. In the embodiment of Figure 38, end-user device 100 includes communication modem 880, memory that includes application program store 830 and application credential and policy store 810, application execution environment 850, and application policy control 820. Communication modem 880 enables end-user device 100 to communicate over at least a first access network. Application program store 830 stores a run-time application program. Application credential and policy store 810 stores a known-application credential associated with a known application program and a known application access network policy associated with the known-application credential. In some embodiments,

IPR2025-01572
Apple EX1002 Page 105

the run-time application credential is stored with the run-time application program. In some embodiments, the known-application credential is a security certificate, signature, or hash for the known application program. In some embodiments, end-user device 100 is further configured to obtain the known-application credential from a network element by way of a secure data connection between end-user device 100 and the network element.

[00276] Application execution environment 850 retrieves the run-time application program from memory and executes it, determines a run-time application credential associated with the run-time application program, and associates the run-time application credential with a run-time communication activity comprising a run-time application program's use of or intended use of the first access network. Application policy control 820 receives the run-time application credential, receives information associated with the run-time application communication activity, and determines whether the run-time application credential matches the known-application credential. If so, application policy control 820 causes the known application access network policy to be applied to the run-time application communication activity.

[00277] In some embodiments, end-user device 100 is further configured to provide the run-time application credential to a network element by way of a secure data connection between end-user device 100 and the network element. In some embodiments, end-user device 100 is further configured to receive information from the network element indicating the validity of the run-time application credential. In some embodiments, end-user device 100 is further configured to receive the information about the application policy from the network element by way of a secure data connection between end-user device 100 and the network element.

[00278] In some embodiments, end-user device 100 protects particular elements (e.g., software) from unauthorized user modification or unauthorized application program modification. For example, in some embodiments, end-user device 100 stores the known-application credential and the known application access network policy in a secure location. In some embodiments, end-user device 100 performs various functions,

IPR2025-01572
Apple EX1002 Page 106

such as: determining the run-time application credential associated with the run-time application program (e.g., the credential-reporting element in the application execution environment); associating the run-time application credential with the run-time application communication activity (e.g., the credential-reporting element in the application execution environment); receiving the run-time application credential (e.g., application policy control 820); receiving information indicating the run-time application communication activity (e.g., the application policy control 820); determining if the run-time application credential matches the known-application credential (e.g., the application policy control 820); causing the known application access network policy to be applied to the run-time application communication activity (e.g., application policy control 820 instructing either the run-time controller element of the application execution environment 850 or the application policy enforcement element in the communications stack 860).

[00279] In some embodiments, the run-time application communication activity is an attempted access or successful access to access network 10 by the run-time application program, and the known application access network policy specifies allowing the access, blocking the access, limiting the access, or accounting for the access.

[00280] In some embodiments, the run-time application communication activity is an attempted access or successful access to an access network by the run-time application program, and the known application access network policy specifies a usage notification policy for notifying the user of the attempted or successful access. In some embodiments, the usage notification policy is configured to present to a user through user interface 1697 an access network service usage breakdown showing the service usage for the run-time application program. In some embodiments, the usage breakdown includes a breakdown by application. In some embodiments, the usage breakdown includes a breakdown by network type. In some embodiments, the usage breakdown includes a breakdown by both application and network type. In some embodiments, the usage breakdown includes a breakdown by network type. In some embodiments, the usage breakdown includes a roaming network breakdown. In some embodiments, the usage breakdown includes a breakdown by roaming network usage and by application.

IPR2025-01572
Apple EX1002 Page 107

[00281] In some embodiments, the usage notification policy is configured to present to a user through user interface 1697 a warning of the potential rate of service usage for the known application program. In some embodiments, the usage notification policy is configured to present to a user through user interface 1697 an offer to purchase service for the run-time application program. In some embodiments, the usage notification policy is configured to present to a user through user interface 1697 an indication of how much of a service allowance allocated to the known application program has been used or is remaining to be used.

[00282] In some embodiments, the run-time application communication activity is an attempt to execute or successful execution of the run-time application program, and the known application access network policy specifies allowing execution of the run-time application program, blocking execution of the run-time application program, or notifying the user of the attempted or successful execution.

[00283] In some embodiments, end-user device 100 is further configured with second access modem 890 to communicate with a second access network, and the run-time application communication activity comprises a run-time application program's use of or attempted use of the first access network or the second access network. In some embodiments, the known application access network policy settings or instructions differ based on whether end-user device 100 is connected to the first access network or to the second access network.

[00284] In some embodiments, user interface 1697 provides a user of end-user device 100 with input capability to modify access network service according to user preference and to receive access network service notifications. In some embodiments, user interface 1697 accepts user inputs for modifying access network policy, such as limiting access by one or more applications or access to one or more network destinations. In some embodiments, user interface 1697 accepts user inputs for choosing or modifying a service plan.

[00285] In some embodiments, at least an aspect of the known application access network policy is entered by a device user through user interface 1697. In some

IPR2025-01572
Apple EX1002 Page 108

embodiments, at least an aspect of the known application access network policy is obtained from a network element.

[00286] In some embodiments, the memory is further configured to store an unknown application access network policy to be applied to the run-time application communication activity when the run-time application credential does not match the known-application credential. In some such embodiments, the application policy decision agent is further configured to determine if the run-time application credential does not match the known-application credential, and, if the run-time application credential does not match the known-application credential, cause the unknown application access network policy to be applied to the run-time application communication activity.

[00287] In some embodiments, end-user device 100 further comprises a policy enforcement agent (e.g., either a run-time controller element of application execution environment 850 or application policy enforcement element 862 in communications stack 860) configured to apply the known application access network policy to the run-time application communication activity and to cause the known application access network policy to be applied to the run-time application communication activity. In some embodiments, the known application access network policy is applied to the run-time application communication activity by providing an instruction to the policy enforcement agent. In some embodiments, the policy enforcement agent (e.g., the run-time controller element of application execution environment 850 or application policy enforcement element 862 in communications stack 860) applies the known application access network policy at the application layer of a device operating system. In some embodiments, the policy enforcement agent applies the known application access network policy at the library or framework layer of a device operating system. In some embodiments, the policy enforcement agent applies the known application access network policy by interacting with communications stack 860 or modifying communications stack traffic flows. In some embodiments, the policy enforcement agent applies the known application access network policy at the kernel or low level OS layer of an operating system of end-user device 100.

IPR2025-01572
Apple EX1002 Page 109

[00288] Figure 39 illustrates an example embodiment wherein end-user device 100 is capable of connecting to Internet 12 through more than one access network (e.g., wireless access network 822 and wireless access network 824). In some embodiments, end-user device 100 is further configured with a second access modem to enable end-user device 100 to communicate over a second access network, and the run-time application communication activity includes a run-time application program's use of or intended use of the first access network or the second access network, and the usage notification policy is configured to provide a user notification that is dependent on which network end-user device 100 is connected to.

End-User Device Agent Verification

[00289] It may be advantageous in some embodiments to validate particular agents on the end-user device that assist in the provisioning and/or management of device-assisted services. In some embodiments, end-user device 100 includes one or more verification agents that may be used to validate one or more device-assisted services agents. There are many possible device-assisted agents that may be verified, such as, for example: a usage reporting agent (e.g., an agent that reports aggregate or finer (e.g., per-service or classification) measures of access network usage by the end-user device), a usage counting agent (e.g., an agent that reports counts of access network usage by the end-user device), a policy enforcement agent, a notification agent, a policy decision agent, a network state agent, a kernel communication agent, a user interface agent, a persistence agent (e.g., an agent that reads or writes from a data store, such as a local memory), a plan catalog agent, a service controller communication agent, a tethering detection agent, a time-of-day agent (e.g., an agent that manages a policy based on time of day), a kernel agent, or an analytics agent. Examples of agents are shown in Figure 2 and other figures and are described herein.

[00290] There are a number of ways in which the verification agent can validate a device-assisted services agent, including, for example: by performing a hash operation, by performing a checksum operation, by determining whether a digital signature is valid, by performing a fingerprint, by generating a random challenge and checking a response by the device-assisted services agent to the challenge, by extracting features from the

IPR2025-01572
Apple EX1002 Page 110

agent for analysis by an artificial intelligence element (e.g., a support vector machine, a hidden Markov model, a decision tree, or a decision forest), etc. In some embodiments, the verification agent sends a verification message to the service controller with information about the results of the verification operation. In some embodiments, the verification message contains information about the integrity status of one or more of the device-assisted services agents. In some embodiments, the verification message comprises a hash, where the hash is the result of one or more of: a hash operation on a kernel component, a hash operation on a system component, a hash operation on an application. In some embodiments, the verification message comprises a hash that is a combination of two or more hashes. In some embodiments, the verification message comprises a salted hash. In some embodiments, the end-user device receives a verification result from the service controller. In some embodiments, the end-user device takes an action based on the verification result (e.g., blocks, allows, rate-limits, or delays an access to the access network by the end-user device; quarantines the end-user device; provides a notification to a user of the end-user device; heals a device-assisted services agent; etc.).

[00291] Figure 40 illustrates an example embodiment of a procedure that a service controller may use to verify a software component on an end-user device based on a verification message from the end-user device. At step 1230, the service controller receives a verification message from the end-user device. In some embodiments, the verification message comprises the result of a hash operation performed by the end-user device. At step 1232, the service controller processes the verification message to obtain a software identifier. In some embodiments, the software identifier is a credential, such as a program identifier, a name, a signature, a certificate, a hash, or any other identifier that uniquely identifies the software. At step 1234, the service controller determines whether the software identifier matches an entry in a locally-stored list of valid software identifiers. If the software identifier matches an entry in the locally-stored list of valid software identifiers, the process ends at step 1238, or, in some embodiments, the service controller takes an action (e.g., sends a message to the carrier, sends a message to the end-user device, initiates a notification to a user of the end-user device, etc.). If the

IPR2025-01572
Apple EX1002 Page 111

software identifier does not match an entry in a locally-stored list of valid software identifiers, then at step 1236 the service controller takes an action (e.g., generates a fraud event, takes a countermeasure such as, for example, blocking the end-user device from the access network, notifies the carrier, sends a message to the end-user device, etc.).

[00292] In some embodiments, one or more agents on end-user device 100 comprise software components that are associated with installed-agent credentials. In some such embodiments, an agent associated with an installed-agent credential cannot be modified, updated, or replaced unless the software purporting to be a modification, update, or replacement is associated with a credential that matches the installed-agent credential. An installed-agent credential may comprise an agent kernel software being present with a proper signature, certificate, or hash result; an agent framework software being present with a proper signature, certificate, or hash result; or an agent application software being present with a proper signature, certificate, or hash result.

Fraud Detection and Mitigation

[00293] In some embodiments, service controller 122 (using, e.g., fraud server 129) is configured to detect fraudulent, or potentially fraudulent, activities by end-user device 100. There are several ways service controller 122 can detect fraud, including, for example, by observing whether service processor 115 exhibits expected behavior; by determining whether device-generated usage reports indicate fraudulent use of the access network resources; by examining the contents of trusted reports (e.g., reports from a trusted or secure source) of end-user device 100's data usage; by comparing contents of non-secure device-based usage reports to contents of trusted usage reports; by comparing end-user device 100's usage to expected usage based on population statistics; by detecting SIM card irregularities that may indicate attempts to steal sponsored services. In some embodiments, service controller 122 obtains a trusted measure of end-user device 100's service usage and uses the trusted measure, alone or in combination with another measure, to determine whether end-user device is properly implementing a policy that should be in place.

[00294] In some embodiments, service controller 122 applies a policy error

IPR2025-01572
Apple EX1002 Page 112

detection procedure to generate a fraud score, wherein the fraud score indicates a level of confidence or a likelihood that the analyzed activity or set of activities is fraudulent. In some embodiments, service controller 122 (using, e.g., fraud server 129) determines whether data usage by end-user device 100 is fraudulent by using what may be called a "layered" or "tiered" approach. In some such embodiments, service controller applies at least two tests to determine whether end-user device 100 is behaving fraudulently. In some such embodiments, a trusted service policy implementation is verified by service controller 122 by performing at least two of the following operations in conjunction with a multi-step service usage analysis procedure: (a) comparing a trusted access network usage records with the usage limitations expected to be in place if the service policy is being properly implemented, (b) comparing a trusted service usage measure to a non-secure (e.g., device-generated) service processor-based service usage measure, (c) comparing a first device service processor service usage measure against a second device service processor service usage measure, and (d) comparing a device service usage measure against a population statistic for the device-based service usage measure.

[00295] Figure 41 illustrates an example embodiment of a layered approach that service controller 122 (or another suitable network element) can use to assess the likelihood that end-user device 100 (e.g., service processor 115) is behaving fraudulently. At step 2750, service controller 122 receives a notification from a network element that a data session has started. The notification may be, for example, a "GPRS attach" message from SGSN 2230, or a "data session started" message from GGSN 2240, AAA or RAIDUS 2242, or API 2244 (or OCS 2246), etc. Service controller 122 sets a timer or waits for some amount of time for service processor 115 to authenticate. If service processor 115 fails to start or complete the authentication procedure at step 2752, then at step 2754, service controller 122 takes an action. The action may be, for example, one or more of the following: generate a fraud alert, notify a user of end-user device 100, notify a network element, notify a network administrator, block end-user device 100 from accessing access network 10, block an application on end-user device 100 from accessing access network 10, direct the device to a quarantine network status in which end-user device 100 can, for example, only access functions generally controlled by the access

IPR2025-01572
Apple EX1002 Page 113

network service provider or the central service provider, etc. If service processor 115 successfully completes the authentication procedure at step 2752, then at step 2756, service controller 122 performs one or more additional fraud tests. At step 2758, service controller determines whether the results of the tests indicate that end-user device 100 is behaving fraudulently. If the results do not indicate that end-user device 100 is behaving fraudulently, then the process ends at step 2760. If the results do indicate that end-user device 100 is behaving fraudulently, then at step 2762, service controller 122 takes an action, such as generating a fraud alert, notifying a user of end-user device 100, notifying a network element, notifying a network administrator, blocking end-user device 100 from accessing access network 10, blocking an application from accessing access network 10, directing the device to a quarantine network status in which end-user device 100 can, for example, only access functions generally controlled by the access network service provider or the central service provider, etc.

[00296] Figure 42 illustrates a layered approach to fraud detection in accordance with some embodiments. Trusted source 2800 (e.g., a network element, a secure DDR processor on end-user device 100, a third-party, etc.) generates trusted records. In some embodiments, the trusted records include service usage records. In some embodiments, the trusted records also (or instead) include information from trusted source 2800 about the behavior of end-user device 100 (e.g., whether service processor 115 successfully authenticated with service controller 122, whether service processor 115 is sending reports or other communications to service controller 122 in an expected manner, whether end-user device 100's usage of one or more classes (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) is consistently slightly under particular limits that would indicate likely fraud on the part of end-user device 100, etc.). Non-secure source 2802 (e.g., service processor 115 on end-user device 100) generates non-secure records. Trusted source 2800 and non-secure source 2802 send records to record normalization and pre-processing 2804. In some embodiments, trusted source 2800 and non-secure source 2802 send records to record normalization and pre-processing 2804 at regular intervals. In some embodiments, record normalization and pre-processing 2804 or another element of service controller

IPR2025-01572
Apple EX1002 Page 114

122 requests records from trusted source 2800 and non-secure source 2802. Record normalization and pre-processing 2804 time-normalizes and pre-processes the trusted and non-secure records, putting the records into a uniform format. The normalized, pre-processed trusted records and the normalized, pre-processed non-secure records then serve as inputs to a set of N tests, where N is greater than or equal to two. Test 1 2806 and Test N 2808 are illustrated in Figure 42. Each of the N tests outputs a test result that provides an indication of fraud likelihood. The results are inputs to combiner 2810, which processes the test results to generate a fraud score.

[00297] In some embodiments, service controller 122 applies at least two tests, and combiner 2810 generates a fraud score based on the results of the at least two tests. In some embodiments, service controller 122 applies one or more of the following tests to determine the fraud score: (a) determining if service processor 115 is failing to send non-trusted (e.g., device-based) service usage reports even though service controller 122 is receiving trusted reports of end-user device 100's service usage; (b) comparing a trusted service usage measure to a limit or range of usage expected if end-user device 100 is properly implementing a service policy that should be in place; (c) comparing a trusted service usage measure to a non-secure (e.g., device-based) usage measure to determine if the difference between the two usage measures is within a specified tolerance; (d) comparing a non-secure (e.g., device-based) service usage measure to a limit or range of usage expected if end-user device 100 is properly implementing a service policy that should be in place; (e) comparing a classification of end-user device 100 usage to a limit or range of usage expected if end-user device 100 is properly implementing a service policy that should be in place; (f) comparing an aggregation of two or more classifications of end-user device 100 usage to an aggregate limit on usage to determine if the difference between the two measures is within a specified tolerance; (g) comparing a trusted measure of usage of a class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) to a limit or range of usage expected if end-user device 100 is properly implementing a service policy that should be in place; (h) comparing a trusted measure of usage of a class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) to a non-

IPR2025-01572
Apple EX1002 Page 115

secure (e.g., device-based) measure of usage of the same class to determine if the difference between the two measures is within a specified tolerance; (i) comparing a statistical characterization of usage by a population of end-user devices to a trusted measure of end-user device 100's service usage to determine if the difference between the two measures is within a specified tolerance; (j) comparing a statistical characterization of usage of a particular class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) by a population of end-user devices to a trusted measure of end-user device 100's usage of that same class to determine if the difference between the two measures is within a specified tolerance; (k) comparing a statistical characterization of usage by a population of end-user devices to a non-secure measure of end-user device 100's service usage to determine if the difference between the two measures is within a specified tolerance; (l) comparing a statistical characterization of usage of a class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) to a non-secure (e.g., device-based) measure of usage of the same class to determine if the difference between the two measures is within a specified tolerance; (m) comparing detailed class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) usage information in a usage report (trusted or non-secure) to determine whether a policy that should be in place allows the classified activity; (n) determining whether service processor 115 successfully authenticated with service controller 122; (o) determining whether service processor 115 is reporting (e.g., sending heartbeat messages, device reports, etc.) to service controller 122 in an expected manner; (p) determining whether usage of one or more classes (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) is consistently slightly under particular limits that would indicate likely fraud on the part of end-user device 100; (q) comparing an amount or percentage of unknown or unclassified data usage allocated by service processor 115 to a particular class to an expected amount or percentage of unknown or unclassified data usage, where the expected amount or percentage is determined using information from a trusted source (e.g., a web crawler, domain object model, etc.).

IPR2025-01572
Apple EX1002 Page 116

[00298] The outputs of the N tests may be pass/fail indicators or values (e.g., integer, binary, real numbers, etc.). In some embodiments in which the outputs of the N tests are pass/fail indicators, combiner 2810 determines a fraud score of "pass" or "fail" (e.g., combiner 2810 generates one fraud score (e.g., a discrete value such as 0) if the result is "pass" and a different fraud score (e.g., a different discrete value such as 1) if the result is "fail"). In some embodiments, the fraud score is "pass" if each of the N individual test results indicates the associated test was passed. In some embodiments, the fraud score is "fail" if at least one of the N individual test results indicates that the associated test was failed. In some embodiments, the fraud score is "pass" if at least M individual test results indicate the associated tests were passed, where M is less than N. In some embodiments, the fraud score is "fail" if M or more individual test results indicate the associated tests were failed. As will be appreciated by a person having ordinary skill in the art in view of the disclosures herein, there are many other ways to combine the individual test results and determine the fraud score, and the examples above are not meant to be limiting.

[00299] In some embodiments, the output of each of the N tests is a value. In some embodiments, combiner 2810 performs a linear combination of the N individual test results. In some embodiments, combiner 2810 scales one or more of the N test results before performing a combination (linear or otherwise).

[00300] In some embodiments, each output value is between a minimum value and a maximum value (e.g., between 0 and 1, or between values A and B, inclusive, etc.), and the maximum value is associated with a high likelihood of fraudulent behavior by end-user device 100. In some embodiments, each output value is between 0 and 1, and each output value represents a probability of fraudulent behavior on the part of end-user device 100. In some such embodiments, combiner 2810 multiplies the individual test result values to generate the fraud score. In some embodiments, combiner 2810 applies a weighting factor to one or more of the N test results before multiplying them. As will be appreciated by a person having ordinary skill in the art in view of the disclosures herein, there are many other ways to combine the individual test results and determine the fraud score, and the examples above are not meant to be limiting.

IPR2025-01572
Apple EX1002 Page 117

[00301] In some embodiments, a high fraud score is associated with a high likelihood of fraudulent behavior on the part of end-user device 100. In some such embodiments, if the fraud score generated by combiner 2810 based on the results of N initial tests is greater than (or greater than or equal to) a threshold, service controller 122 generates a fraud alert. In some embodiments, if the fraud score generated by combiner 2810 based on the results of N initial tests, where N is less than the maximum number of tests available, is greater than (or greater than or equal to) a threshold, additional tests are run. In some embodiments, one or more additional tests are added to the set of tests selected initially (e.g., the value of N is increased, and additional tests are selected and included). In some embodiments, at least one of the one or more additional tests is more computationally-expensive than one or more of the tests in the initial set of N tests.

[00302] In some embodiments in which a high fraud score is associated with a high likelihood of fraudulent behavior on the part of end-user device 100, if the fraud score generated by combiner 2810 based on the results of N initial tests, where N is less than the maximum number of tests available, is greater than (or greater than or equal to) a threshold, a different set of N tests is selected and run. In some embodiments, the different set of N tests includes one or more of the tests run in the initial set of N tests. In some embodiments, at least one of the tests in the different set of N tests is more computationally-expensive than one or more of the tests in the initial set of N tests.

[00303] In some embodiments, a low fraud score is associated with a high likelihood of fraudulent behavior on the part of end-user device 100. In some such embodiments, if the fraud score generated by combiner 2810 based on the results of N initial tests is less than (or less than or equal to) a threshold, service controller 122 generates a fraud alert. In some embodiments, if the fraud score generated by combiner 2810 based on the results of N initial tests, where N is less than the maximum number of tests available, is less than (or less than or equal to) a threshold, additional tests are run. In some embodiments, one or more additional tests are added to the set of tests selected initially (e.g., the value of N is increased, and additional tests are selected and included). In some embodiments, at least one of the one or more additional tests is more computationally-expensive than one or more of the tests in the initial set of N tests.

IPR2025-01572
Apple EX1002 Page 118

[00304] In some embodiments in which a low fraud score is associated with a high likelihood of fraudulent behavior on the part of end-user device 100, if the fraud score generated by combiner 2810 based on the results of N initial tests, where N is less than the maximum number of tests available, is less than (or less than or equal to) a threshold, a different set of N tests is selected and run. In some embodiments, the different set of N tests includes one or more of the tests run in the initial set of N tests. In some embodiments, at least one of the tests in the different set of N tests is more computationally-expensive than one or more of the tests in the initial set of N tests.

[00305] In some embodiments, one of the N tests indicates whether service processor 115 successfully completed the authentication procedure with service controller 122. In some embodiments, a failure of service processor 115 to complete the authentication procedure with service controller 122 results in a fraud score that indicates end-user device 100 is likely behaving fraudulently (e.g., an automatic "fail" or a fraud score that indicates a high likelihood of fraud). In some embodiments, the result of one or more tests is a quantized value associated with a likelihood of error (e.g., fraud) or a likelihood of non-error (e.g., no fraud), and the overall pass/fail criterion is based on a combination of one or more of the quantized values.

[00306] In some embodiments, service controller 122 applies different sets of N tests at different times. For example, in some embodiments, service controller 122 applies a set of N tests including more computationally expensive tests on occasion or periodically. In some embodiments, service controller 122 varies the value of N at various times. In some embodiments, service controller 122 regularly applies a small or modest set of tests, and then occasionally or periodically applies a larger set of tests. In some such embodiments, the larger set of tests includes one or more tests that are more computationally expensive than tests in the smaller set (e.g., tests that require processing of flow data records, discussed below).

[00307] In some embodiments, if the fraud score indicates a policy implementation error (e.g., likely fraudulent behavior by end-user device 100), service controller 122 takes an action comprising one or more of: generating a fraud alert; flagging end-user

IPR2025-01572
Apple EX1002 Page 119

device 100 or a user associated with end-user device 100 for further evaluation; charging for end-user device 100's usage at a pre-determined rate associated with end-user device 100 being in a fraudulent state; notifying a user of end-user device 100; notifying a network administrator; quarantining end-user device 100 or a user's access to the access network; suspending end-user device 100 or a user of end-user device 100 from the access network.

Fraud Detection Based on Service Processor Behavior

[00308] Fraudulent or potentially fraudulent activity by end-user device 100 can be detected by service controller 122 by observing the behavior of end-user device 100 after service processor 115 has been authenticated. In some embodiments, detecting fraud comprises ensuring that service control device link 1691 and service control server link 1638 are operating correctly, and there is no break in a continuous heartbeat authentication sequence.

[00309] In some embodiments, service processor 115 sends periodic or occasional device-based usage data reports (UDRs) to service controller 122. The UDRs contain information about end-user device 100's data usage. For example, the UDRs may indicate how many bytes of data associated with a particular application, such as a map application, or service, such as a music streaming service, end-user device used since the last report, or during a particular time period. In some embodiments, service processor 115 sends the UDRs in response to a request from service controller 122. In some embodiments, service controller 122 generates a fraud alert if, after having been authenticated, service processor 115 fails to send device-based usage reports when expected or requested by service controller 122, or when service processor 115 sends device-based usage reports at unexpected or improper times. In some embodiments, service controller 122 generates a fraud alert if it receives UDRs from service processor 115 after receiving a "data session stopped" trigger from a network element.

[00310] In some embodiments, service controller 122 generates a fraud alert if service processor 115 fails to respond as expected to commands issued by service controller 122. In some embodiments, service controller 122 sends a command to service processor 115

IPR2025-01572
Apple EX1002 Page 120

and observes a response from service processor 115. In some embodiments, when fraud is suspected, service controller 122 instructs service processor 115 to apply and enforce policy modifications. Service controller 122 then observes the response of service processor 115 and performs an analysis on information sent by service processor 115 to service controller 122 to determine whether the behavior of end-user device 100 is indicative of fraud.

[00311] In some embodiments, service controller 122 directs service processor 115 to change a setting of end-user device 100. If the setting change ordinarily would cause a deterministic behavior change in the operation of an end-user device that is operating according to an established policy, service controller 122 may determine that end-user device 100 is operating fraudulently if service controller 122 does not observe that end-user device 100's behavior has changed in the expected manner. As an example, service controller 122 might suspend end-user device 100's use of a sponsored service (i.e., a service for which a sponsor entity subsidizes an end-user device's access to that service). If end-user device 100 continues to use the sponsored service after service controller 122 suspended end-user device 100's use of the sponsored service, service controller 122 may conclude that the access is fraudulent.

[00312] In some embodiments, service controller 122 changes a parameter to cause end-user device 100 to modify its behavior and potentially also to change particular settings of end-user device 100. For example, service controller 122 might communicate to service processor 115 a lower maximum data rate at which end-user device 100 is allowed to send data over the access network. If end-user device 100 continues to send data at a rate above the newly-imposed maximum data rate, service controller 122 may conclude that end-user device 100 is operating fraudulently. In some embodiments, parameter changes are constructed, for example, from rules or by building a reaction model for a user population, where the reaction model learns to distinguish legitimate activity from fraudulent behavior.

Fraud Detection Using Trusted Usage Measures/Records

[00313] Fraudulent or potentially fraudulent activity by end-user device 100 can be

IPR2025-01572
Apple EX1002 Page 121

detected by examining trusted measures or records of data usage by end-user device 100. In some embodiments, a network element (e.g., service usage reconciliation and fraud detect 642 or fraud server 129) examines the content of usage reports from a trusted source to determine whether end-user device 100 is operating within the policies that should be in place. The usage reports may indicate a variety of information, including, for example, one or more of: a "bulk" measure of aggregate data usage, destinations accessed, network state (e.g., time of day, network busy state, network congestion state, etc.), type of network (e.g., 2G, 3G, 4G, WiFi, home, roaming, etc.), etc. In some embodiments, the trusted records contain information about end-user device 100's data use associated with a class of service activities, where the class is a particular application, a group of applications, a particular network destination, a group of network destinations, a network type, etc. For example, the trusted records may contain one or more of: record start time, record end time, information identifying the class, the amount of data use associated with the class, etc.

[00314] There are several possible sources of trusted records, including network elements, end-user device 100, and third-party sources. Records from network elements are generally trusted because it is difficult for unauthorized parties to obtain access to the records themselves or the network elements that generate the records, particularly if some or all of the security measures disclosed herein are in place. Examples of network elements that can produce trusted records are: gateways (e.g., GGSN 2240, SGSN 2230, PDSN, routers, switches, etc.), a home agent, proxy servers, a charging gateway system, a mediation element (e.g., mediation 22210), a reconciliation element (e.g., reconciliation server 131), a billing element (e.g., central billing 1619, carrier billing 139), a AAA element (e.g., access network AAA server 1621), and other network elements.

[00315] End-user device 100 can also generate trusted records if it includes a secure device data record (DDR) processor and a secure protocol for the sending of reports from the secure DDR processor to service controller 122. The use of secure DDRs is described in detail in United States patent application number 13/247,998, which is entitled "Secured Device Data Records" and is incorporated herein by reference.

IPR2025-01572
Apple EX1002 Page 122

[00316] Third-party sources can also provide trusted records if measures are in place to verify the reports. Examples of third-party sources that can provide trusted records are: partner service destination servers (e.g., search sites, advertisement sites, application service sites, shopping sites, content sites, gaming sites, e-mail sites, etc.), enterprise customer networks, etc. Third-party sources may provide such information as usage reports, site visits, transaction reports, ad view reports, economic benefit reports, usage credit increase instructions, etc.

[00317] In some embodiments, using data usage reports from a trusted source, a network element determines whether end-user device 100's usage, as given by a trusted usage measure is within a limit or range of usage behavior expected if an applicable policy is in place. For example, in some embodiments, the network element determines whether the bulk usage by end-user device 100 is no higher than a maximum amount specified by a policy that should be in place. In some embodiments, the network element determines whether end-user device 100's use of a particular class (e.g., an application, a group of applications, a network destination, a group of network destinations, network type, etc.) is within data usage limits specified in the control policy that should be in place. In some embodiments, the network element determines whether end-user device 100's use of a particular class is allowed under the control policy that should be in place. As will be now be appreciated by one of ordinary skill in the art in view of the disclosures herein, there are many ways that a network element can use information in reports from a trusted source to verify that end-user device 100 is operating in compliance with policies that should be in place, and the examples given above are not meant to be limiting.

Fraud Detection Using Non-Secure Device-Based Usage Measures/Records

[00318] In some embodiments, service processor 115 is not capable of generating and sending secure DDRs. Instead, service processor 115 is capable only of generating and sending non-secure records (e.g., UDRs) of end-user device 100's data usage. In such cases, an unscrupulous user might attempt to hack end-user device 100 so that the reports it sends contain information that is more favorable to the user than it should be, e.g., by reporting less data usage (either aggregate or of a class) than end-user device 100

IPR2025-01572
Apple EX1002 Page 123

actually used or by reporting data usage that should be accounted as usage under a subscriber-paid service plan as usage of a sponsored service. In some embodiments, service controller 122 uses device-based usage measures to detect when a user attempts to tamper with service processor 115 in order to have usage of one service reported incorrectly (e.g., as usage of a different class, as usage of a sponsored service when it is actually part of a subscriber-paid plan, etc.). In some embodiments, service controller 122 compares usage measures in device-based (e.g., non-secure) reports to corresponding usage measures in a report from a trusted source.

[00319] In some embodiments, service controller 122 generates a fraud alert if it receives UDRs from end-user device 100, but the UDRs indicate end-user device 100's usage is beyond a charging policy limit. In some embodiments, if service controller 122 receives UDRs from end-user device 100, but the charging codes in those UDRs do not correspond to charging codes for the currently-allowed active services (e.g., the charging codes indicate that end-user device 100 is using data or a class for which it is not authorized, etc.), service controller 122 generates a fraud alert.

[00320] In some embodiments, service controller 122 examines the content of device-based usage reports (e.g., reports generated by service processor 115 and sent to service controller 122) to verify that service processor 115 is properly classifying services. In some embodiments, service controller 122 determines whether applications being used or destinations being accessed by end-user device 100 are authorized under a service plan associated with end-user device 100. In some embodiments, service controller 122 examines the content of device-based usage reports to determine whether end-user device 100 imposed a service control that was supposed to be in place (e.g., a cap on usage; a speed of usage (such as a maximum rate); an amount of usage of background or foreground data; state modifiers such as time-of-day, network busy state, network type (e.g., home, roaming, WiFi, cellular, etc.); quality-of-service limits, etc.).

[00321] In some embodiments, service controller 122 examines the content of device-based usage reports to verify that the service usage measures being reported by end-user device 100 are compliant with the access network policy or policies that should

IPR2025-01572
Apple EX1002 Page 124

be in place. In some embodiments, service controller 122 determines whether one or more of the following measures are within limits imposed by a policy that should be in place: bulk (e.g., aggregate) usage; usage of a class (e.g., an application, a group of applications, a network destination (e.g., IP address, domain address, etc.), a group of network destinations, etc.); application-specific usage that includes transaction-based single-application service or multi-application service; background usage; foreground usage; usage that is identified by a time-of-day, network-busy-state, quality-of-service, or network-type state modifier; roaming usage; usage associated with specific content (e.g., streaming video, streaming audio, etc.); usage based on a specific layer 3/4 protocol (e.g., TCP, UDP, and/or a Layer 7 protocol (e.g., IGMP, RTMP, RSTP, etc.)).

[00322] In some embodiments in which service processor 115 tracks end-user device 100's use of a class (e.g., an application, a group of applications, a network destination, a group of network destinations, network type, etc.), service controller 122 examines the content of device-based usage reports to determine whether end-user device 100 is properly identifying and allocating data usage associated with the class. As is described in detail in several previous applications listed in the "Cross Reference to Related Applications" section (including U.S. patent publication 2010/0198698, filed January 27, 2010 and entitled "Adaptive Ambient Services"), classifying data usage in the dynamic (e.g., non-static) environment of the Internet can be challenging. For example, a class may include access to a particular web site. Service processor 115 should count, as usage of the class, end-user device 100's access to the collection of URLs associated with the web site, but not access to other network destinations and/or applications not associated with the web site. Although it is possible to create, at any point in time, a comprehensive list of all content associated with the web site, a problem arises whenever the web site changes (e.g., links or URLs are changed, content from other web sites is included or removed, etc.), because the list of associated addresses/domains and access list policies will be inaccurate if it is not updated immediately after the change.

[00323] Several of the patent applications listed in the "Cross Reference to Related Applications" section of this document, including United States patent application

IPR2025-01572
Apple EX1002 Page 125

number 13/253,013, entitled "System and Method for Providing User Notifications" and incorporated by reference herein, disclose ways to track changes in the Internet to facilitate providing, for example, service plans with different classes, sponsored services, etc. One way to track changes is to use search engine/web crawler techniques to create and update a catalog of content sources, destinations (e.g., advertisement servers, network domains, etc.) etc. that are associated with a class. As would be understood by a person of ordinary skill in the art, a web crawler is a computer program that browses the web in a methodical, automated way. Web crawlers are also known as ants, automatic indexers, bots, web spiders, web robots, or web scutters. Web crawlers may be used to copy, check, or validate links on web sites. A web crawler may start with a list of URLs to visit. As the crawler visits these URLs, it identifies all the hyperlinks in the page and adds them to the list of URLs to visit. The new list is sometimes called the crawl frontier. URLs from the crawl frontier are then recursively visited according to a set of policies that specify which pages to visit, how often to re-visit those pages, etc.

[00324] The immediate identification and propagation to all service processors of all changes in every web site associated with every sponsored service or every class within all service plans can be difficult. Therefore, in some embodiments, when end-user device 100 engages in service activities associated with a class (e.g., sends or receives data using a particular application that is itself a class, or using an application from a defined set of applications comprising a class; or accesses a particular network destination that is itself a class, or accesses a particular network destination that is in a class comprising a set of network destinations; or uses a particular network type, etc.), and in the course of using data within the class end-user device 100 is directed to a destination that service processor 115 does not know or is unclassified, service processor 115 grants a temporary access "lease." Under the lease, access to, for example, certain unknown or unclassified destinations is allowed (e.g., for a particular amount of data, for a particular amount of time, etc.) but monitored until the unclassified or unknown application or destination can be reclassified as allowed or disallowed. A lease temporarily allows unknown or unclassified activities to take place within the class under the theory that such activities may be the legitimate result of a change in an Internet

IPR2025-01572
Apple EX1002 Page 126

destination included in the class, and, therefore, it would be undesirable to block these activities or to allocate data access costs associated with them to a "bulk" usage category or to a different class when they should be allocated to the class.

[00325] Service controller 122 can use information from a web crawler/search engine (e.g., the crawl frontier) to assess whether service processor 115 is likely correctly allocating data usage to particular classes. In some embodiments, service controller 122 determines whether service processor 115 is allocating a reasonable amount of unknown or unclassified data usage to the class based on web crawler results. For example, if the web crawler results indicate that, at a particular point in time or on average, approximately 80 percent of content available at or through a particular web site is known (e.g., has a URL that alone indicates it is part of the class, has a URL that indicates it is from an ad server or another so-called known, benign domain, the content of which is unlikely to be accessed fraudulently by a user, etc.), and 20 percent of the content is unknown (e.g., not known to be part of the class, not a known, benign domain, etc.), service controller 122 may determine that end-user device 100 is likely operating fraudulently if only 50 percent of the data usage allocated by service processor 115 is known to be associated with the web site, and the other 50 percent of the data usage allocated by service processor 115 to the class is associated with unknown or unclassified content or destinations. Such a result may indicate that service processor 115 has been hacked and is improperly allocating data usage to the class.

[00326] In some embodiments, service controller 122 determines whether device-based usage reports indicate that service processor 115 is likely fraudulently allocating data usage to a sponsored service. For example, in some embodiments, service controller 122 determines how much of the data usage service processor 115 is allocating to a sponsored service is known to be associated with the sponsored service and how much is not known to be associated with the sponsored service. In some embodiments, service controller 122 determines (e.g., based on web crawler or similar data) whether service processor 115 is allocating too much unknown or unclassified data usage to a sponsored service. In some embodiments, service controller 122 assesses whether service processor 115 is properly granting leases (e.g., by determining whether the leases are of an

IPR2025-01572
Apple EX1002 Page 127

appropriate duration, are terminated properly, etc.). In some embodiments, service controller generates a fraud alert if the UDRs indicate that end-user device is improperly classifying disallowed destinations (e.g., web sites, URLs, etc.) as part of a sponsored service.

[00327] In some embodiments, service controller 122 compares usage counts in carrier-based usage reports, or usage reports from another trusted source, to usage counts in UDRs from end-user device 100. In some embodiments, if the difference between the usage counts in the two reports is not within a tolerance (e.g., an amount of data, a percentage, etc.), service controller 122 generates a fraud alert. In some embodiments, if the counts in the reports agree, and the charging codes in the UDRs are correct, but the UDRs indicate that service processor 115 has incorrectly categorized (e.g., classified) the data usage, service controller 122 generates a fraud alert. In some embodiments, if the counts in the reports are in agreement, but the usage rate (e.g., units of data per unit of time) within a service component (e.g., a class) or within a service activity is greater than a rate limit set by the control policy, service controller 122 generates a fraud alert.

[00328] In some embodiments, service controller 122 generates a fraud alert if a comparison between the device-based UDRs and carrier-based (or other trusted) usage reports indicates that end-user device 100 consistently under-reports its usage of data in a particular class (e.g., an application, a group of applications, a destination, a group of destinations, etc.). Such underreporting may indicate that service processor 115 is substituting usage counts from a higher-priced service for the counts associated with a lower-priced or sponsored service (e.g., service processor 115 is reporting more usage of the lower-priced service and less usage of the higher-priced service). Such "skimming" can occur, for example, within a single service, across multiple services, across multiple time periods, or in other ways or combinations of these ways.

[00329] In some embodiments, service controller 122 generates a fraud alert if the UDRs from service processor 115 indicate that end-user device 100's usage of a service, component, or activity is abnormal when compared to a hard rate limit, such as an allowed usage per hour, day, or week, or an expected rate limit, such as a rate limit

IPR2025-01572
Apple EX1002 Page 128

imposed on streaming services.

[00330] In some embodiments, service controller 122 compares a usage rate of end-user device 100 to the "average" end-user device usage rate, which it determines using a statistical model of usage data associated with a specific service plan or component of a service plan (e.g., a class) by a population or sub-population of devices. In some such embodiments, service controller 122 performs what is known in the art as a k-nearest neighbor classification, using the usage rate to identify whether end-user device 100 is potentially behaving fraudulently. As would be understood by a person having ordinary skill in the art, the k-nearest neighbor classification may be trained by learning vector quantization (LVQ) using tunable training parameters such as, for example, the time window of data usage, usage rate, etc.

[00331] In some embodiments, service controller 122 may or may not generate a fraud alert upon detecting a particular condition. For example, if the usage counts contained in trusted reports and UDRs from service processor 115 are in agreement, but end-user device 100's usage rate, in terms of units of data per unit of time, deviates significantly from the usage rate of the "average" user, it could mean that service processor 115 has been tampered with or otherwise compromised. Alternatively, however, it could mean simply that the usage patterns for that service activity or service component are changing, or that end-user device 100 is being used legitimately, but in an unusual manner as compared to how most end-user devices are used. A change in usage patterns could result, for example, if the service plan to which end-user device 100 is subscribed adds streaming content, such as video or audio, and a user is among the first to take advantage of the new content. In some embodiments, service controller 122 may simply flag the activity as potentially fraudulent, or it may wait until it has performed additional analysis to make a decision regarding whether service processor 115's behavior is likely fraudulent.

[00332] In some embodiments, service controller 122 determines a second measure of a network state to confirm that end-user device is reporting the correct network state in its charging reports. In some embodiments, service controller 122 (or another suitable

IPR2025-01572
Apple EX1002 Page 129

network function) obtains the network state as determined using a group of devices. In some embodiments, service controller 122 (or another suitable network function) characterizes sub-network portions (e.g., base stations, base station sectors, geographic areas, RANs, etc.) based on a population of end-user devices connected to that sub-network portion.

[00333] In some embodiments, service controller 122 determines a second measure of device access behavior for a given network state to ensure end-user device 100 is implementing the correct controls. In some embodiments, the second measure is from a network element. In some embodiments, the second measure is from a secure DDR processor on end-user device 100. In some embodiments, the second measure is from a second monitor point within end-user device 100. In some embodiments, the second measure is "good customer feedback" from a third party source.

[00334] In some embodiments, service controller 122 compares a trusted (e.g., network-based, secure DDR, or third-party) measure of the device's service usage to a device-based (e.g., service-processor-based) measure of the device's service usage. In some embodiments, one or both of the trusted service usage measures and the device-based service usage measures include a classification of service usage based on application. In some embodiments, one or both of the service usage measures include a classification of service usage based on network destination or network service identifier. In some embodiments, one or both of the service usage measures include a classification of service usage based on network type (e.g., roaming, home, cellular, WiFi, etc.). In some embodiments, one or both of the service usage measures include a classification of service usage based on time of day. In some embodiments, one or both of the service usage measures include a classification of service usage based on QoS class. In some embodiments, one or both of the service usage measures include a classification of service usage based on geography. In some embodiments, one or both of the service usage measures include a classification of service usage based on a roaming network.

[00335] In some embodiments, a trusted service policy implementation is verified by comparing a first device-based service processor service usage measure against a second

IPR2025-01572
Apple EX1002 Page 130

device-based service processor service usage measure. In some embodiments, one or both service processor usage measures include a classification of service usage based on application. In some embodiments, one or both service processor usage measures include a classification of service usage based on network destination or network service identifier. In some embodiments, one or both service processor usage measures include a classification of service usage based on network type. In some embodiments, one or both service processor usage measures include a classification of service usage based on time of day. In some embodiments, one or both service processor usage measures include a classification of service usage based on QoS class. In some embodiments, one or both service processor usage measures include a classification of service usage based on geography. In some embodiments, one or both service processor usage measures include a classification of service usage based on a roaming network.

[00336] Figure 43 illustrates an example embodiment of a service controller reconciliation processing procedure that may be used to detect fraud using information from an end-user device 100 and information from a second source. Service processor 115 (not shown) or an application on end-user device 100 (not shown) generates usage measures 2300. Based on usage measures 2300, end-user device 100 sends first usage records to service controller 122, or service controller 122 requests first usage records from end-user device 100. Service controller 122 processes the first usage records in device usage record pre-processing 2310. In some embodiments, device usage record pre-processing 2310 modifies the format of the first usage records to facilitate one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation operations performed within the service controller system. In some embodiments, device usage record pre-processing 2310 observes the first usage records and time stamps and time synchronizes, time aligns, or time aggregates multiple first usage records so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation purposes. Service controller 122 stores the first usage records in device usage records 2320.

[00337] A second source (not shown) generates or provides second service usage

IPR2025-01572
Apple EX1002 Page 131

measures 2370. In some embodiments, the second source is a network element, such as a mediation element, a gateway, a real-time reporting element, a charging element, a billing element, or the like. In some embodiments, the second source is a database. In some embodiments, the second source is a roaming partner network element. In some embodiments, the second source is an element on end-user device 100 that generates secure device data records. In some embodiments, the second source is a partner network destination that provides information about customer usage of or transactions with that destination. In some embodiments, the second source is an application on end-user device 100.

[00338] Based on the second service usage measures, the second source sends second usage records to service controller 122, or service controller 122 obtains the second usage records from the second source. Service controller 122 processes the second usage records in record normalization, time reconciliation and pre-preprocessing 2360. In some embodiments, record normalization, time reconciliation and pre-preprocessing 2360 modifies the format of the second usage records to facilitate one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation operations performed within the service controller system. In some embodiments, record normalization, time reconciliation and pre-preprocessing 2360 observes the second usage records and time stamps and time synchronizes, time aligns, or time aggregates multiple second usage records so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation purposes. Service controller 122 stores the second usage records in second source usage records 2350.

[00339] Service controller 122 applies reconciliation and verification processing algorithms 2340 to reconcile records in device usage records 2320 with records in second source usage records 2350 and to validate records in device usage records 2320. Service controller 122 stores information based on the results of reconciliation and verification processing algorithms 2340 in data warehouse 2330.

IPR2025-01572
Apple EX1002 Page 132

[00340] In some embodiments, reconciliation and verification processing algorithms 2340 reconcile detailed classifications of service usage off of a bulk service usage accounting and onto a finer classification of service usage accounting. For ease of explanation, the finer classifications of service usage accounting are referred to herein as "micro charging data records" or "micro-CDRs." In some embodiments, reconciliation and verification processing algorithms 2340 accomplish charging for detailed classifications of service usage by providing a detailed micro-CDR charging code identifier in the micro-CDR usage record communicated to the carrier network mediation or billing system (e.g., operator data mediation 2380). In some embodiments, reconciliation and verification processing algorithms 2340 accomplish charging for a detailed classification of service usage by mediating out (or subtracting) the amount of service usage reported in the micro-CDR from the amount of service usage accounted to bulk service usage. In some embodiments, reconciliation and verification processing algorithms 2340 sends charging data records (e.g., CDRs, micro-CDRs, etc.) to operator data mediation 2380.

[00341] In some embodiments, reconciliation and verification processing algorithms 2340 perform a fraud analysis using information from one or both of second source usage records 2350 and device usage records 2320. In some embodiments, reconciliation and verification processing algorithms 2340 compares usage records associated with a specific device or user credential from one or both of second source usage records 2350 and device usage records 2320 to determine if service usage is outside of pre-defined service usage policy behavior limits. In some embodiments, reconciliation and verification processing algorithms 2340 compares service usage information associated with a specific device or user credential from one or both of second source usage records 2350 and device usage records 2320 to determine if a pre-defined service usage limit has been reached or exceeded. In some embodiments, reconciliation and verification processing algorithms 2340 compares service usage information associated with a specific device or user credential from one or both of second usage records 2350 and device usage records 2320 to determine if the specific device or user is exhibiting a service usage behavior that is outside of pre-defined statistical limits as compared to the service usage behavior of a device or user population. In some embodiments,

IPR2025-01572
Apple EX1002 Page 133

reconciliation and verification processing algorithms 2340 stores the results of its fraud analysis in data warehouse 2330. In some embodiments, reconciliation and verification processing algorithms 2340 sends fraud alerts to operator CRM system 2390 (e.g., a carrier fraud processing system, carrier personnel, a device user, a system administrator, etc.).

[00342] In some embodiments, the second usage records comprise information from multiple other measures or reports. In some embodiments, the second usage records are based on information, measures, or reports from end-user device 100. In some embodiments, the second usage records are based on information, measures, or reports from other end-user devices. In some embodiments, the second usage records are determined based on information, measures, or reports from one or more network elements (e.g., a base station, the RAN, the core, or using device-assisted means, etc.).

[00343] In some embodiments, the second usage records comprise a measure of bulk (e.g., aggregate or unclassified) data usage by end-user device 100. For example, in some embodiments, the second usage records comprise a bulk usage report, specific to end-user device 100, generated by the network, by an application service provider, or by a server. In some embodiments, the second usage records are based on information in one or more previous reports sent by end-user device 100.

[00344] In some embodiments, the second usage records comprise information associated with the access network state. In some embodiments, the second usage records are determined from network state tagged information. In some embodiments, the second usage records comprise information from a device data record (DDR), which may indicate the network busy state and the network type. In some embodiments, the second usage records are determined from DDR network state tagged information.

[00345] In some embodiments, the second usage records comprise information from flow data record. In some embodiments, the flow data record (FDR) reports a detailed level of service usage classification that indicates service usage broken down by network source or destination (e.g., domain, URL, IP address, etc.) and possibly one or more ports and protocols. In some embodiments, the FDR reports a detailed level of service usage

IPR2025-01572
Apple EX1002 Page 134

classification that indicates usage broken down by device user application or OS application. In some embodiments, the FDR reports a detailed level of service usage classification that indicates service usage broken down by time of day, network congestion state or service QoS level. In some embodiments, the FDR reports a detailed level of service usage broken down by network type (e.g., 2G, 3G, 4G, WiFi, home, roaming, etc.). In some embodiments, the FDR reports a detailed level of service usage broken down by home or roaming network.

[00346] In some embodiments, the FDRs are sourced from a network element capable of classifying traffic (e.g., a deep packet inspection [DPI] gateway, a proxy server, a gateway or server dedicated to a given service classification, a good customer feedback source described elsewhere herein, etc.). In some embodiments, the second usage records are derived from a device service monitor. In some embodiments, the second usage records are derived from a trusted device service monitor. In some embodiments, the trusted device service monitor is located in a secure execution environment on the device that cannot be accessed by a user or user installed application software.

[00347] In some embodiments, the second usage records allow service controller 122 to determine whether the access behavior of end-user device 100, given the network state, indicates that end-user device 100 is implementing the correct policy controls. In some embodiments, service controller 122 confirms that service processor 115 is reporting the correct network state in its data usage reports. In some embodiments, a network element determines the correct network state based on a group of devices. The information is reported to service controller 122 or another suitable network function. Service controller 122 (or other suitable network function) characterizes portions of the sub-network (e.g., base stations, base station sectors, geographic areas, radio access network (RAN), etc.) based on the population of end-user devices connected to that sub-network portion. The network element can also gather network busy-state measures from network equipment, such as from base stations or by sampling the RAN, to determine the second measure.

[00348] In some embodiments, the second usage records provide information about a

IPR2025-01572
Apple EX1002 Page 135

cap on the aggregate amount of data usage by end-user device 100. Service controller 122 verifies that the total data usage by end-user device 100, as reported in the first usage records, does not exceed the cap. If the first usage records provide data usage amounts for individual services used by end-user device 100, service controller 122 verifies that the sum of the usage amounts for the individual services does not exceed the cap.

[00349] In some embodiments, the network classifies FDRs to known service components, determines credits of classified usage for each service component, ensures that the service component usage does not exceed specified limits (or matches end-user device reports for the component), and checks whether the sum of the components matches the bulk measure.

[00350] There are several potentially fraudulent circumstances that may be detected by service controller 122 using one or more of the embodiments disclosed herein, such as the example embodiment illustrated in Figure 43. In some embodiments, service controller 122 generates a fraud alert if it receives carrier-based usage reports from a network element and UDRs from service processor 115, but the usage counts contained in the reports are not in agreement within a specified tolerance. In order to generate a fraud alert under these circumstances, in some embodiments service controller 122 accounts for unsent usage reports that may still be on end-user device 100.

[00351] Figure 44 illustrates an exemplary embodiment with network system elements that can be included in a service controller system (e.g., service controller 122) to facilitate a device-assisted services (DAS) implementation and the flow of information between those elements. Figure 44 shows the flow of information to facilitate reconciliation of device-generated data usage records with network-generated (e.g., wireless network carrier-generated) data usage records associated with an end-user device, such as end-user device 100.

[00352] Carrier-generated charging data records (CDRs) or real-time reporting records (RTRs) (or other real-time or near-real-time usage record formats such as, e.g., flow data records (FDRs), batch processed usage records, continuous usage record event feeds or SMS formatted usage record messages) flow from carrier 2650 (which can be, e.g., a real

IPR2025-01572
Apple EX1002 Page 136

time reporting system, a network gateway, a network usage charging system element, a AAA, an HLR, a billing element, etc.) to load balancer 2652 to CDR/RTR filtering element 2654.

[00353] In some embodiments, load balancer 2652 selects one of many CDR/RTR processing threads that are available in the service controller information processing system. In some embodiments, the processing thread is an asynchronous software or firmware program running on a gateway or server CPU. In some embodiments, the processing thread is a virtual machine processing thread that exists in a resource pool of gateway or server CPUs or virtual machines, which may include geographically separated or redundant resource pools. As illustrated in Figure 44, each processing thread includes the functional steps of CDR/RTR filtering 2654, JMS queue 2656, CDR/RTR processor 2658 and the interface to CDR/RTR database 2660. In some embodiments, processing threads are asynchronous in that they are initiated when load balancer 2652 directs one or more CDR/RTR data transfers to the thread and terminated when the processed CDR/RTR information has been processed and deposited into CDR/RTR database 2660. Note that Figure 44 shows only one of potentially many available CDR/RTR processing threads.

[00354] CDR/RTR filtering element 2654 selects the records that are associated with devices that include a device client that communicates with the service controller (e.g., the device client can be a service processor configured to provide service usage notification updates, on-device service plan purchase or activation with UI options display and user selection actions, device-assisted access control policy enforcement, device-assisted service usage charging policy enforcement, device-assisted service notification messages, etc.). In some embodiments, devices supporting DAS are identified by device credentials or user credentials that are communicated to the service controller as described herein, where the device credential or user credential are members of a device group or user group that is managed by the service controller.

[00355] In some embodiments, CDR/RTR filtering element 2654 may be used advantageously to quickly receive and acknowledge a CDR/RTR record to provide

IPR2025-01572
Apple EX1002 Page 137

asynchronous functionality because of real-time processing requirements, server processing thread scalability and maintainability requirements, or server processing thread geographic redundancy requirements. In some embodiments, filtering eliminates unnecessary load on JMS queue 2656 and/or CDR/RTR database 2660. CDR/RTR filtering element 2654 places the records from end-user devices known to be configured with a device client (e.g., a service processor configured to provide service usage notification updates, on-device service plan purchase or activation with UI options display and user selection actions, device-assisted access control policy enforcement, device-assisted service usage charging policy enforcement, device-assisted service notification messages, etc.) that communicates with the service controller through Java messaging service (JMS) queue 2656. In some embodiments, CDR/RTR filtering element 2654 filters out device records for devices that may have a form of service processor 115, but service processor 115 has not properly authenticated with the service controller 122. In some embodiments, the device clients that are known to be configured with a device client that communicates with service controller 122 are determined by looking up a device credential or user credential associated with CDRs or RTRs in a device group or user group management database.

[00356] JMS queue 2656 buffers the CDR/RTR information remaining after CDR/RTR filtering 2654 and allocates one or more CDRs/RTRs to a service usage processing thread in CDR/RTR processor 2658. In some embodiments, JMS queue 2656 is a persistent queue. In some embodiments, JMS queue 2656 is a primary messaging system between service controller applications.

[00357] CDR/RTR processor 2658 retrieves the records from JMS queue 2656, transforms the records, and stores them in CDR/RTR database 2660. In some embodiments, CDR/RTR processor 2658 is an application or a process thread. In some embodiments, CDR/RTR processor 2658 pulls a CDR/RTR record from JMS queue 2656, transforms the record, and stores the transformed record in CDR/RTR database 2660 in one transaction in order to provide fault tolerance in the case of system failure. In some embodiments, CDR/RTR processor 2658 formats the CDR/RTR information to provide a common service usage information format to facilitate one or more of service

IPR2025-01572
Apple EX1002 Page 138

usage processing, reporting, analysis, comparison, mediation and reconciliation operations performed within the service controller system. In some embodiments, CDR/RTR processor 2658 observes CDR/RTR time stamps and time synchronizes, time aligns, or time aggregates multiple CDR/RTR reports so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison, mediation and reconciliation purposes.

[00358] In some embodiments, end-user devices capable of DAS reporting (e.g., devices configured with a device client that communicates with the service controller, such as service processor 115 described herein) connect periodically or on occasion to usage reporting gateway 2672 to report their data usages. In some embodiments, DAS reporting information includes but is not limited to one or more of user service plan purchase or activation selection choices, device user service policy configuration preference selections (e.g., user-generated service policy assignments for applications, websites, network types, or home/roaming policies), DAS service usage reports, DAS device policy state reports, DAS software environment integrity reports, and other reports.

[00359] In some embodiments, DAS device usage reports and analytics flow from carrier device network 2668 (e.g., devices configured with service processors 115 that are in communication with the service controller) to load balancer 2670 to usage reporting gateway 2672. In some embodiments, load balancer 2670 selects one of many usage reporting processing threads that are available in the service controller information processing system. In some embodiments, the usage reporting processing thread is an asynchronous software or firmware program running on a gateway or server CPU. In some embodiments, the usage reporting processing thread is a virtual machine processing thread that exists in a resource pool of gateway or server CPUs or virtual machines, which may include geographically separated or redundant resource pools. As illustrated in Figure 44, each usage reporting processing thread consists of the functional steps of usage reporting gateway 2672, JMS queue 2674, report processor 2676, and the interface to usage report database 2678. In some embodiments, usage reporting processing threads

IPR2025-01572
Apple EX1002 Page 139

are asynchronous in that they are initiated when load balancer 2670 directs one or more usage reporting data transfers to a thread and terminated when the processed usage reporting information has been processed and deposited into usage report database 2678. Note that Figure 44 shows only one of potentially many available usage reporting processing threads.

[00360] Usage reporting gateway 2672 accepts reports from devices configured with a device client (e.g., service processor 115 configured to provide service usage notification updates, on-device service plan purchase or activation with UI options display and user selection actions, device assisted access control policy enforcement, device assisted service usage charging policy enforcement, device assisted service notification messages, etc.) that communicates with service controller 122 and places the reports on JMS queue 2674. In some embodiments, usage reporting gateway 2672 only accepts device reports from device service processors 115 that have authenticated with the service controller system (e.g. service controller 122). In some embodiments, usage reporting gateway 2672 only accepts device reports from device service processors 115 configured with device credentials or user credentials that are members of a device group or user group that is managed by service controller 122. In some embodiments, usage reporting gateway 2672 rejects reports from end-user devices without authenticated service processors. In some embodiments, usage reporting gateway 2672 is an application or a process thread. In some embodiments, usage reporting gateway 2672 quickly receives and acknowledges end-user device reports. In some embodiments, usage reporting gateway 2672 provides asynchronous functionality that is advantageous to support real-time processing requirements.

[00361] In some embodiments, end-user device 100 is authenticated before reports are put onto JMS queue 2674. In some embodiments, JMS queue 2674 is a persistent queue. In some embodiments, JMS queue 2674 is a primary messaging system between service controller applications.

[00362] Report processor 2676 retrieves reports from JMS queue 2674, transforms the reports, and stores the transformed reports in usage report database 2678. In some

IPR2025-01572
Apple EX1002 Page 140

embodiments, report processor 2676 is an EAI. In some embodiments, report processor 2676 retrieves reports from JMS queue 2674, transforms the reports, and stores the transformed reports in usage report database 2678 in a single transaction in order to provide fault tolerance in case of system failure. In some embodiments, report processor 2676 formats the device usage report information to provide a common service usage information format to facilitate one or more of service usage processing, reporting, analysis, comparison mediation and reconciliation purposes internal processing and comparison within the service controller system. In some embodiments, report processor 2676 observes device usage report time stamps and time synchronizes, time aligns or time aggregates multiple device usage reports so that a more consistent measure of usage with a common time reference can be achieved within the service controller system for one or more of service usage processing, reporting, analysis, comparison mediation and reconciliation purposes.

[00363] In some embodiments, CDR/RTR filtering 2654, CDR/RTR processor 2658, report processor 2676, and usage reporting gateway 2672 share a host.

[00364] In some embodiments, micro-CDR generator 2680 retrieves records from CDR/RTR database 2660 and retrieves reports from usage report database 2678. In some embodiments, micro-CDR generator 2680 determines a service usage amount for a micro-CDR service usage classification, assigns a usage accounting identifier to the micro-CDR report that identifies the usage as being accounted to a device user for the device associated with a device credential or user credential, and reports this amount of service usage to the carrier network 2666 (in the exemplary embodiment of Figure 44, through JMS queue 2662 and FTP or publisher 2664). In some embodiments, micro-CDR generator 2680 determines a service usage amount for a micro-CDR service usage classification, assigns a usage accounting identifier to the micro-CDR report that identifies the usage as being accounted to a service sponsor, and reports this amount of service usage to carrier network 2666. In some embodiments the micro-CDR for the sponsored service usage report also includes an identifier for a device credential or user credential. In some embodiments, the amount of service usage accounted for in the micro-CDR is mediated or reconciled off of a device or user bulk service usage

IPR2025-01572
Apple EX1002 Page 141

accounting. In some embodiments, micro-CDR generator 2680 sends micro-CDRs to JMS queue 2662. In some embodiments, FTP or publisher 2664 retrieves micro-CDRs from JMS queue 2662 and pushes the micro-CDRs to carrier 2666.

[00365] In some embodiments, fraud analyzer 2682 retrieves records from CDR/RTR database 2660. In some embodiments, fraud analyzer 2682 retrieves reports form usage report database 2678. In some embodiments, fraud analyzer 2682 retrieves micro-CDRs from micro-CDR generator 2680. In some embodiments, fraud analyzer 2682 performs a fraud analysis using information from one or more of CDR/RTR database 2660, usage report database 2678, and micro-CDR generator 2680. In some embodiments, fraud analyzer 2682 compares usage records associated with a specific device or user credential from one or more of CDR/RTR database 2660, usage report database 2678, and micro-CDR generator 2680 to determine if service usage by that device is outside of pre-defined service usage policy behavior limits. In some embodiments, fraud analyzer 2682 compares service usage information associated with a specific device or user credential from one or more of CDR/RTR database 2660, usage report database 2678, and micro-CDR generator 2680 to determine if a pre-defined service usage limit has been reached or exceeded by that device. In some embodiments, fraud analyzer 2682 compares service usage information associated with a specific device or user credential from one or more of CDR/RTR database 2660, usage report database 2678 and micro-CDR generator 2680 to determine if the specific device or user is exhibiting a service usage behavior that is outside of pre-defined statistical limits as compared to the service usage behavior of a device or user population. In some embodiments, fraud analyzer 2682 stores the results of its fraud analysis in data warehouse 2694. In some embodiments, fraud analyzer 2682 sends fraud alerts to carrier network 2666.

Fraud Detection for Time-Based Service Plans

[00366] In some embodiments, a service plan in effect for end-user device 100 is a time-based service plan (e.g., access network costs associated with a particular service or application are not charged to the user, or are charged to the user at a reduced rate during a particular time period). In some such embodiments, an agent on end-user device 100 detects fraudulent or potentially fraudulent activities by determining whether the time or

IPR2025-01572
Apple EX1002 Page 142

time zone setting on end-user device 100 is correct or within a tolerance. Figure 45 illustrates an example procedure to detect when a user of end-user device 100 attempts to alter end-user device 100's use of a time-based service plan by modifying the time setting on end-user device 100.

[00367] At step 1060, an agent (e.g., policy control agent 1692, service monitor agent 1696, policy implementation agent 1690, etc.) on end-user device 100 obtains the actual time. In some embodiments, the agent obtains the actual time from a trusted source. In some embodiments, the trusted source is an NTP server. In some embodiments, the trusted source is a cell tower. In some embodiments, the agent obtains the actual time based on information about a cell tower location. In some embodiments, the agent obtains the actual time based on information from a GPS receiver. In some embodiments, the agent obtains the actual time based on a geo-located IP address. At step 1062, the agent compares the time setting on the device (the device time) to the actual time. At step 1064, the agent determines if the difference between the actual time and the device time is within a tolerance. In some embodiments, the tolerance is set by portal user 102. If the difference is within the tolerance, the process ends at step 1068. If the difference is not within the tolerance, the agent takes an action at step 1066. In some embodiments, the action is to generate a fraud alert. In some embodiments, the action is to adjust the time setting on end-user device 100. In some embodiments, the action is to use the actual time to enforce a policy (e.g., a control policy, a charging policy, or a notification policy). In some embodiments, the action is to take a countermeasure, such as, for example, to block, delay, rate-limit, or quarantine access to the access network by end-user device 100. In some embodiments, the action is to provide a notification to a user of end-user device 100. In some embodiments, the action is to send a message to service controller 122.

[00368] Figure 46 illustrates an example embodiment of a procedure to detect when a user of end-user device 100 attempts to alter end-user device 100's use of a time-based service plan by modifying the time zone setting of end-user device 100. At step 1070, an agent (e.g., policy control agent 1692, service monitor agent 1696, policy implementation agent 1690, etc.) on end-user device 100 obtains the actual time zone. In

IPR2025-01572
Apple EX1002 Page 143

some embodiments, the agent obtains the actual time zone from a trusted source. In some embodiments, the trusted source is an NTP server. In some embodiments, the trusted source is a cell tower. In some embodiments, the agent obtains the actual time zone based on information about a cell tower location. In some embodiments, the agent obtains the actual time zone based on information from a GPS receiver. In some embodiments, the agent obtains the actual time zone based on a geo-located IP address. At step 1072, the agent compares the time zone setting on the device to the actual time zone. At step 1074, the agent determines if the difference between the actual time zone and the device time zone is within a tolerance. In some embodiments, the tolerance is set by portal user 102. If the difference is within the tolerance, the process ends at step 1078. If the difference is not within the tolerance, the agent takes an action at step 1076. In some embodiments, the action is to generate a fraud alert. In some embodiments, the action is to adjust the time zone setting on end-user device 100. In some embodiments, the action is to use the actual time zone to enforce a policy (e.g., a control policy, a charging policy, or a notification policy). In some embodiments, the action is to take a countermeasure, such as, for example, to block, delay, rate-limit, or quarantine access to the access network by end-user device 100. In some embodiments, the action is to provide a notification to a user of end-user device 100. In some embodiments, the action is to send a message to service controller 122.

Additional Fraud Detection Techniques

[00369] Figure 47 illustrates a fraud detection approach in accordance with some embodiments. UDRs (e.g., device-based usage records) are provided to rule-based detection element 2550. In some embodiments, rule-based detection element 2550 includes rules that can be applied to detect fraud scenarios that can be described deterministically. As will now be appreciated by a person having ordinary skill in the art, many of the detection approaches disclosed herein are amenable to being implemented as rules for use by rule-based detection element 2550. For example, a comparison between a policy that is supposed to be in place and information in a usage report associated with end-user device 100, whether the report is device-based or network-based, trusted or non-secure, etc., can easily be expressed as a rule. Examples of potential rules include, but

IPR2025-01572
Apple EX1002 Page 144

are not limited to: whether end-user device 100's bulk usage is below a service plan cap; whether end-user device 100's usage of a particular class (e.g., an application, a group of applications, a network destination, a group of network destinations, etc.) is below a service plan limit; whether end-user device 100's usage of a sponsored service is compliant with the sponsored service policy that should be in place; whether end-user device 100's usage of a particular network, network type, quality-of-service class, etc. is compliant with a control policy that should be in place; whether end-user device 100 failed the authentication procedure; etc.

[00370] In the embodiment of Figure 47, rule-based detection element 2550 also obtains CDRs. In some embodiments, rules in fraud rules 2510 are event driven and are applied to incoming events (e.g., CDRs from the carrier network or UDRs from end-user device) in real time or near-real time. As will be appreciated by a person having ordinary skill in the art in light of the disclosures herein, rule-based detection element 2550 may use only UDRs, only CDRs, or both UDRs and CDRs.

[00371] Figure 48 illustrates a procedure that rule-based detection element 2550 may use to apply rules to detect fraud. At step 2560, rule-based detection element 2550 obtains device events or reports, e.g., UDRs and/or CDRs. At step 2562, rule-based detection element 2550 places the obtained device events in working memory. At step 2564, rule-based detection element 2550 obtains one or more rules and processes the device events using those rules. At step 2566, rule-based detection element 2550 determines whether the results of the processing indicate a fraud event. If so, then at step 2568, rule-based detection element 2550 stores the fraud event in main database 2514. If not, rule-based detection element 2550 returns to step 2560 to begin the procedure again with additional or different records.

[00372] As illustrated in Figure 47, UDRs are also supplied to static analysis element 2552, which generates a fraud score upon detecting potentially fraudulent behavior by end-user device 100. In some embodiments, static analysis element 2552 determines a fraud score using one or more models obtained from a statistical modeling element. In some embodiments, static analysis element 2552 compares end-user device

IPR2025-01572
Apple EX1002 Page 145

100's service usage against a corresponding population statistic for the device-based service usage measure. In some embodiments, these population statistics for the device-based service usage measures include a classification of service usage based on application. In some embodiments, these population statistics for the device-based service usage measures include a classification of service usage based on network destination or network service identifier. In some embodiments, these population statistics for the device-based service usage measures include a classification of service usage based on network type. In some embodiments, these population statistics for the device-based service usage measures include a classification of service usage based on time of day. In some embodiments, these population statistics for the device-based service usage measures include a classification of service usage based on QoS class. In some embodiments, these population statistics for the device-based service usage measures include a classification of service usage based on geography. In some embodiments, these population statistics for the device-based service usage measures include a classification of service usage based on a roaming network.

[00373] Figure 49 illustrates a procedure static analysis element 2552 uses to determine fraud based on a statistical model in accordance with some embodiments. At step 2588, static analysis element 2552 retrieves UDRs from UDR storage 2598 and builds a static classification model. At step 2590, static analysis element 2552 delays the UDRs. At step 2592, static analysis element 2552 checks the data drift. At step 2594, static analysis element 2552 determines whether the data drift is significant. If the drift is not significant, then static analysis element 2552 returns to step 2590, and the UDRs are further delayed. If the drift is significant, then static analysis element 2552 returns to step 2588 and builds a new static classification model. At step 2580, static analysis element 2552 computes the current usage profile for end-user device 100 over the reference time period in the UDRs obtained from UDR storage 2598. At step 2582, static analysis element 2552 classifies end-user device 100's behavior using model 2596. At step 2584, static analysis element 2552 determines whether end-user device 100's behavior should be classified as fraudulent. If so, then at step 2586, static analysis element 2552 stores a fraud score in main database 2514. If, at step 2584, static analysis element 2552

IPR2025-01572
Apple EX1002 Page 146

determines that end-user device 100's behavior should not be classified as fraudulent, then static analysis element 2552 returns to step 2580 to analyze the next UDRs.

[00374] As illustrated in Figure 47, UDRs are also supplied to time-series analysis element 2554, which generates a fraud score upon detecting potentially fraudulent behavior by end-user device 100. As will be appreciated by a person having ordinary skill in the art, a time series is a sequence of data points, typically measured at successive times spaced at uniform time intervals. Time-series analysis comprises methods of analyzing time series data to extract meaningful statistics and other characteristics of the data. A time-series model generally reflects the fact that observations close together in time are more closely related (e.g., correlated) than observations that are further apart. In addition, time-series models often make use of the natural one-way ordering of time so that values for a given period are expressed as deriving in some way from past values and not from future values. In some embodiments, time-series models are used to detect significant changes in an individual subscriber's usage behavior that might indicate fraud. In some embodiments, a time-series model is used to compare current data usage against a past usage trend or to predict future potential fraud based on past usage. A time-series model may model an individual device's data usage, or it may leverage population or subpopulation data.

[00375] Figure 50 illustrates a procedure time-series analysis element 2554 uses to determine fraud based on a time-series model in accordance with some embodiments. At step 2608, time-series analysis element 2554 retrieves UDRs from UDR storage 2598 and builds a time-series model (e.g., a hidden Markov model). At step 2612, time-series analysis element 2554 delays the UDRs. At step 2614, time-series analysis element 2554 checks the data drift. At step 2616, time-series analysis element 2554 determines whether the data drift is significant. If the drift is not significant, then time-series analysis element 2554 returns to step 2612, and the UDRs are further delayed. If the drift is significant, then time-series analysis element 2554 returns to step 2608 and builds a new time-series model. At step 2600, time-series analysis element 2554 collects a sequence of usage data over a reference time period using UDRs obtained from UDR storage 2598. At step 2602, time-series analysis element 2552 computes a distribution of

IPR2025-01572
Apple EX1002 Page 147

hidden states at the end of the sequence using time-series model 2610. At step 2604, time-series analysis element 2554 determines whether end-user device 100's behavior should be classified as fraudulent. If so, then at step 2606, time-series analysis element 2554 stores a fraud score in main database 2514. If, at step 2604, time-series analysis element 2554 determines that end-user device 100's behavior should not be classified as fraudulent, then time-series analysis element 2554 returns to step 2600 to analyze the next UDRs.

[00376] Fraud control center 2516 retrieves fraud data from main database 2514 and performs one or more of the following functions: an aggregate analysis of various fraud metrics (events and/or scores) to determine whether end-user device 100 is likely operating fraudulently; presentation of fraud-related information through a dashboard (e.g., a user interface); and taking an action to mitigate the fraud (e.g., notify a network administrator of a network resource so that further evaluation can take place, increase a billing rate for end-user device 100, notify a user of or subscriber associated with end-user device 100 of the service agreement violation and, if applicable, increased billing rate, via one or more communication media [e.g., service processor 115, device notification client user interface, text message, e-mail message, voicemail, phone call], throttle or suspend end-user device 100's access to the access network, throttle or suspend an application's access to the access network.

[00377] Figure 51 illustrates a fraud detection system that supports rule-based fraud detection and the application of statistical or time-series models in accordance with some embodiments. End-user device 100, equipped with service processor 115, exchanges network traffic with carrier element 2506 (e.g., a AAA server such as access network AAA server 1620, GGSN such as GGSN 2240, etc.). Service processor 115 also sends UDRs to gateway application server 138. Gateway application server 138 sends the UDRs to EAI server 128. In addition to device-based UDRs, EAI server 128 also receives network-based CDRs from RADIUS server 2504. EAI server 128 processes the UDRs and/or the CDRs and stores the processed records in main database 2514 (which may be within database cluster 116). EAI server 128 also sends some or all of the records to fraud server 129. Fraud server 129 includes fraud rules 2510 and fraud models

IPR2025-01572
Apple EX1002 Page 148

2512. Fraud rules 2510 includes one or more rules that fraud server 129 may apply to determine whether to generate a fraud event, as, for example, described in the context of Figure 48. Fraud models 2512 includes one or more models that fraud server 129 may apply to determine whether to generate a fraud score, as, for example, described in the context of Figures SS and TT,

[00378] As illustrated in the embodiment of Figure 51, offline statistical model 2522 retrieves UDRs from main database 2514 and generates models for use by fraud server 129 in determining whether end-user device 100 is operating fraudulently. In some embodiments, offline statistical model 2522 uses population data (e.g., UDRs, CDRs, etc.) to construct group profiles for legitimate subpopulations and for fraudulent subpopulations of end-user devices within the control of service controller 122. In some embodiments, offline statistical model 2522 identifies sudden or long-term trends or global behavior shifts and adapts one or more data models based on those trends or shifts. In some embodiments, offline statistical model 2522 uses on-line learning to refine and train one or more models.

[00379] Fraud server 129 generates fraud events (e.g., fraud alerts) and stores them in main database 2514. Fraud control center 2516 retrieves fraud data from main database 2514. Depending on the content of the fraud data, fraud control center 2516 may display information about the fraud data on dashboard 2518, which, in some embodiments, includes a user interface such as a display. In some embodiments, fraud responder 2520 takes an action based on the fraud data, such as notifying carrier 2506 of fraudulent or potentially fraudulent activity by end-user device 100.

Detection of Fraudulent Use of SIM Cards

[00380] End-user device 100 may contain a "sponsored SIM" card or another credential that allows the device to use a fixed amount of data, possibly associated with a particular service, at a reduced charge or at no charge to the user. Unscrupulous users may attempt to find ways to increase their quantity of free or subsidized data usage with sponsored SIM cards. In some embodiments, service controller 122 detects fraud associated with SIM cards and takes actions to address the fraud.

IPR2025-01572
Apple EX1002 Page 149

[00381] Without loss of generality, in the following related embodiments the terms "SIM card" and "SIM" are used to represent a device credential source. As would be appreciated by one of ordinary skill in the art, other device credential sources (e.g., a soft-SIM, a universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.) can be interchanged with SIM card in many of the embodiments. For example, in embodiments in which a SIM card is moved from one device to another, another type of device credential could be moved instead (e.g., soft SIM, universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.). As another example, when a user tampers with a service processor associated with a SIM, the user could be tampering with a service processor associated with another type of device credential (e.g., soft SIM, universal SIM, an IMSI source, a wireless modem, a phone number source, an IMEI source, an MEID source, a MAC address source, an IP address source, a secure device identifier source, a device secure communication encryption key source, etc.). There are many other examples where the term "SIM" can be exchanged for another source of device credentials, with the examples being too numerous to list and yet evident to one of ordinary skill in the art in the context of the teachings herein.

[00382] In some embodiments, the one or more device credential sources include a SIM card. In some embodiments, service controller 122 can be configured to recognize which end-user device 100 or service processor 115 the SIM is associated with, use the SIM and device association to look up a desired device portion of a wireless access network service policy, and communicate the policy to the appropriate device service processor. In some embodiments, the two different device portions of a wireless access network policy are determined according to a device group or user group service policy definition that includes one or more SIM credentials and/or one or more service processor credentials, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or service processor policies.

IPR2025-01572
Apple EX1002 Page 150

[00383] In some embodiments, service controller 122 is configured to recognize when the SIM card from a first device with a first service processor has been moved to a second device with a second service processor. In some such embodiments, service controller 122 is configured to recognize which device or service processor the SIM is associated with, use the SIM and device association to look up a desired network portion of a wireless access network service policy, and cause the network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments, the two different network portions of a wireless access network policy are determined according to a device group or user group service policy definition that includes one or more SIM credentials and/or one or more service processor credentials, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or network service policy enforcement element policies.

[00384] In some embodiments, the one or more device credential sources include a SIM card. In some embodiments, service controller 122 is configured to detect when a device user has moved the SIM card from a first device configured with a properly configured service processor to a second device that is not configured with a properly configured service processor. In some embodiments, service controller 122 is configured to determine that the first device is configured with a properly configured service processor and communicate a device portion of a wireless access network service policy to the appropriate device service processor. In some embodiments, the device portion of a wireless access network policy is determined according to a device group or user group service policy definition that includes a SIM credential and/or a service processor credential, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or device service processor policies. In some embodiments, service controller 122 is configured to determine that the first device is configured with a properly configured service processor and cause a first network portion of a wireless access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments, service controller 122 is configured to determine that the second device is not configured with a properly configured service processor and cause a second network portion of a wireless

IPR2025-01572
Apple EX1002 Page 151

access network service policy to be implemented or enforced in one or more network service policy enforcement elements. In some embodiments, the device portion of a wireless access network policy is determined according to a device group or user group service policy definition that includes a SIM credential, and these policy definitions are entered in a virtual service provider work station that manages the service controller and/or network service policy enforcement element policies.

[00385] In some of these embodiments, the differences between the first network portion of a wireless access network service policy and the second network portion of a wireless access network service policy can include a difference in network access privileges, a difference in allowable network destinations, a difference in service usage accounting or billing for "bulk" access, a difference in service usage accounting or billing for a classification of access, a difference in service usage accounting rates or billing rates for "bulk" access, a difference in service usage accounting rates or billing rates for a classification of access, a difference in sponsored (ambient) service accounting or billing, a difference in service speed or quality, a difference in which networks the device or user has access to, a difference in the service usage notification that is provided to the end user, a difference in roaming service policies or permissions or accounting/billing rates, a quarantining of the device or user access capabilities, differences between (e.g., disabling or otherwise modifying) one or more features of device operation, or suspending the device from access to the network.

[00386] In some embodiments, a SIM and service processor 115 are associated with a classification of service usage and a corresponding device portion of access network service policy enforcement. Service controller 122 is then responsible for properly authenticating the proper configuration of service processor 115 in association with the SIM in order to determine the appropriate network portion of network access service policy that should be enforced.

[00387] In some embodiments, a SIM and service processor 115 are associated with one or more application-specific services wherein the device network access service has policy elements that are specific to a device software or firmware application. A

IPR2025-01572
Apple EX1002 Page 152

software or firmware application-specific service can include but is not limited to a service with specific policy elements associated with a user application program; an operating system program, library or function; a background application service such as an application update, content caching, software update or other background application service.

[00388] In some embodiments, a SIM and service processor 115 are associated with one or more network-destination-specific services wherein the device network access service has policy elements that are specific to a network destination or resource. A network destination or resource can include but is not limited to a server, gateway, destination address, domain, website or URL.

[00389] In some embodiments, a SIM and service processor 115 are associated with any combination of a device application, network destination or resource; a type of network; a roaming condition (e.g., a home or roaming network); a time period; a level of network congestion; a level of network quality-of-service (QoS); and a background or foreground communication.

[00390] In some embodiments, a SIM and service processor 115 are associated with one or more sponsored services (also referred to herein as ambient services), wherein a portion or all of the service usage accounting for one or more classifications of service usage are accounted to, charged to, or billed to a service sponsor rather than the device user or party who pays for the user service plan. The portion of service that is sponsored can be all of the device access or a portion or classification of the device access. In some embodiments, the classification of the sponsored portion of service (e.g., the identification of the portion of the device's use of the access network that should be allocated to the service sponsor) is accomplished on the device with service processor 115. In some embodiments, the classification of the sponsored portion of service is accomplished in the network using DPI elements, gateway elements, server elements, proxy elements, website elements or web service elements. In some embodiments, the classification of the sponsored portion of service is accomplished with a classification policy implemented by a combination of a service processor on the device (e.g., steering

IPR2025-01572
Apple EX1002 Page 153

a classification of service to a given network element via a re-direction, re-route, or tunnel [e.g. secure SSL, VPN, APN or other tunnel protocol]) and one or more network elements (e.g., DPI elements, gateway elements, server elements, proxy elements, website elements or web service elements). In some embodiments, the portion of service that is sponsored includes service for one device application or a group of device applications. In some embodiments, the portion of service that is sponsored includes service for a network destination or resource, a server or website, or a group of network destinations, servers or websites. In some embodiments, the portion of service that is sponsored includes service on a specific type of network. In some embodiments, the portion of service that is sponsored includes service on a home network or a roaming network. In some embodiments, the portion of service that is sponsored includes service during a time period. In some embodiments, the portion of service that is sponsored includes service for a certain range of network congestion. In some embodiments, the portion of service that is sponsored can include service for a certain range of network QoS. In some embodiments, the portion of service that is sponsored includes service for a network background or foreground data communication. In some embodiments, the portion of service that is sponsored includes any combination of device application, network destination or resource, a type of network, a roaming condition (e.g., home or roaming network), a time period, a level of network congestion, a level of network QoS, and a background or foreground communication.

[00391] In some embodiments, a SIM (or other source of user credential or device credential, as explained previously) is installed in or present in association with a device configured with a device service processor configuration that provides access network policy enforcement. In such embodiments, one or more network elements can implement or enforce a network-based portion of access network policy enforcement, and service processor 115 can be configured to implement or enforce a device-based portion of access network policy enforcement. In some embodiments, one or more SIM credentials can be used at least in part to identify the network-based portion of access network policy. In some embodiments, one or more SIM credentials can be used at least in part to identify the device-based portion of access network policy.

IPR2025-01572
Apple EX1002 Page 154

[00392] In some embodiments that include a SIM module policy association, the policy enforcement includes one or more of access control policy enforcement, service usage limit, access accounting policy enforcement, and access service user notification policy enforcement. In some embodiments, the access control policy enforcement includes one or more of allowing, limiting, blocking, deferring, delaying or traffic shaping device network access for "bulk" access (e.g., "not classified" access), or one or more specific classifications of access network service activities. In some embodiments, the access accounting policy enforcement includes one or more of counting an amount of "bulk" (e.g., "unclassified") access network service usage, or counting an amount of access network service usage for one or more specific classifications of access network service activities. In some embodiments, the access service notification policy enforcement includes one or more of notifying an end user when a pre-defined service usage condition occurs for "bulk" (e.g. "unclassified") access network service usage or notifying an end user when a pre-defined service usage condition occurs for one or more specific classifications of access network service activities. Examples of specific classifications of access network service activities include access by an application or OS function, access to one or more network destinations or network resources (such as a web site, domain, IP address or other address identifier, URL, socket tuple, network server, network route or APN, network gateway or proxy, network content source or sub-network). Additional examples of specific classifications of access network service activities include device access to network services with different QoS service levels. In some embodiments, a portion of the policies associated with specific classifications of access network service are implemented or enforced with a device-based service processor, and other portions of access network service policy are enforced in one or more network-based elements.

[00393] In some embodiments in which one or more network elements implement or enforce a network-based portion of access network policy enforcement and a device service processor is configured to implement or enforce a device-based portion of access network policy enforcement, one or more device SIM credentials are identified and used at least in part to determine the policies enforced by the network. In such embodiments, service processor 115 can be relied upon to implement or enforce certain aspects of

IPR2025-01572
Apple EX1002 Page 155

access network service policy that are not implemented or enforced in the network.

[00394] In some embodiments, a first portion of access network service policy is determined at least in part by one or more SIM credentials and is implemented by one or more network elements, and a second portion of access network service policy is intended to be implemented by a device-based service processor, but the SIM is installed in a device that is not configured with a service processor capable of implementing the second portion of access network service policy. In some such embodiments, a network element identifies whether the SIM is installed in a device that is configured with a service processor capable of implementing the second portion of access network service policy intended to be implemented on the device. In some embodiments, the identification is accomplished by a network system that implements one or more of the following device configuration detection and network policy selection functions: (1) Identify when a SIM whose credentials are used at least in part to identify a network-based portion of access network policy is installed in a device configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, and provision a first network-based service policy in one or more network-based policy enforcement elements that implement or enforce access network service policy; (2) Identify when a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device that is not configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy and implement a second network-based service policy in one or more network-based policy enforcement elements that implement or enforce access network service policy.

[00395] In some embodiments, when it is determined that a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, a network-based service policy provisioning system provisions a first network-based service policy into one or more network elements (e.g., programs or sends the policy to one or more network elements) and also provisions a device-based service policy into a device service

IPR2025-01572
Apple EX1002 Page 156

processor. In some embodiments, when it is determined that a SIM whose credentials are used at least in part to identify the network-based portion of access network policy is installed in a device that is not configured to include a service processor capable of implementing or enforcing a device-based portion of access network service policy, a network-based service policy provisioning system provisions a second network-based service policy into one or more network elements, and there is no policy provisioning for a device-based service processor.

[00396] Such embodiments are advantageous, for example, when a device-based service processor is capable of implementing or enforcing a network access service policy that has fine grain classification aspects that are not otherwise implemented or enforced in the network. For example, in some embodiments a SIM is installed in a first device configuration that includes a device-based service processor (e.g., service processor 115) capable of classifying access network service usage associated with one or more device software applications and enforcing a policy for access control, service limit, access accounting or access service notification for that classification. In this case, a first set of network-based access network service policies may be provisioned into the network elements that implement or enforce access network service policy. If the same SIM is installed in a second device configuration that does not include the described service processor capability, a second set of network-based access network service policies may be provisioned into the network elements that implement or enforce access network service policy. In such embodiments, the first device configuration can include a trusted access control or service limit policies in service processor 115 that determine the network access allowances for one or more applications, and the first network service policies are configured to facilitate this device-based application access control or service limitation. In contrast, the second device configuration, having no service processor, has no trusted access control or service limitation policies, and therefore the second network service policies may be configured in a manner that allows access only if the service plan or service account associated with the SIM (or second device or SIM user) includes permissions for "bulk" access, "unclassified" access, or access that is classified by the network and not by the device.

IPR2025-01572
Apple EX1002 Page 157

[00397] In some embodiments, the second network service policies are configured to modify the classification of network access services in accordance with capabilities that exist only in the network without the assistance of a device-assisted classification component.

[00398] In some embodiments, the second network service policies include a second access service accounting or charging rate that is different than the access service accounting or charging rate of the first network service policies. For example, the method of service accounting or service charging to the end user in the case where the SIM is installed in a device configuration that includes a service processor capability (e.g., the device is capable of performing service classification, accounting, control or notification functions) can be different than the method of service accounting or service charging to the end user in the case where the SIM is installed in a device configuration that does not include the service processor capability. For example, if the SIM is installed in a device configuration that includes a service processor capability, a given application (e.g., social networking application, email application, search application, voice application, news application, etc.) might have a first service accounting or charging policy defining a first charging measure (e.g., time-based usage for an application, website, content type, service type QoS class; or e.g., megabyte-based usage for an application, website, content type, service type QoS class, etc.) and/or first charging rate (e.g., $X per minute; or e.g., $Y per megabyte, etc.) when the device configuration includes a service processor capability, whereas when the SIM is not installed in a device configuration that includes a service processor capability, all traffic may be rated in the same manner (e.g., time-based or megabyte-based), potentially with a higher price. In some embodiments, when the SIM is not installed in a device configuration that includes a service processor capability, the device network access permissions are altered, or the device's communications may be quarantined or blocked.

[00399] In some embodiments, when a SIM is installed in a device with a first device configuration, service processor 115 is configured to differentially treat one or more classifications of access network service activities based on network congestion level, time of day, QoS level or background/foreground access (e.g., background content

IPR2025-01572
Apple EX1002 Page 158

caching or background upload of device/user analytics, background software or OS updates, background application/server communications, etc.), but the same SIM can alternatively be installed in a device without such service processor capabilities (e.g., a device with a second device configuration). In such an embodiment, one or more of the network-based portions of access control or service limitation policy, network-based portion of accounting or charging policy, or network-based portion of user notification policy can be varied depending on whether the SIM is installed in a device with the first device configuration or the second device configuration. For example, if the SIM is recognized by the network in association with the first device configuration, a lower accounting rating or service usage price can be applied to traffic that is (i) allocated to background status, (ii) is controlled based on network congestion level, (iii) is controlled based on time of day, (iv) is controlled based on a lower QoS classification allowance, etc., whereas if the SIM is recognized by the network in association with the second device configuration, a single, potentially higher accounting rating or service usage price can be applied. In some embodiments, if the SIM is recognized by the network in association with the second device configuration the device network access permissions can be altered, or the device's communications can be quarantined or blocked.

[00400] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor service usage charging capability, one or more network elements are configured to zero-rate the device access (i.e., the one or more network elements will not apply the service usage accounting recorded by one or more network elements to the user's bill), and user service accounting or charging is turned over to a service controller that receives service usage accounting or charging information from the service processor.

[00401] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, one or more network elements are configured to zero-rate the device access (i.e., the one or more network elements will not apply the service usage accounting recorded by one or more network elements to the user's bill), and user service

IPR2025-01572
Apple EX1002 Page 159

accounting or charging is turned over to one or more proxy gateway/servers configured to account or charge for device service usage.

[00402] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the one or more proxy gateway/servers perform additional traffic access control or service limitation policy implementation or enforcement for the one or more classifications of service usage.

[00403] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the one or more proxy gateway/servers perform additional service usage classification for the purpose of service usage accounting, access control, service limiting or user notification.

[00404] In some embodiments, when a SIM is determined by a network element to be installed in a device configuration that does not include a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, network elements other than the proxy gateway/servers account for service usage, potentially at a different rate than when a SIM is determined by a network element to be installed in a device configuration that includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications.

[00405] In some embodiments in which the device configuration includes a service processor capability to route, re-direct or otherwise steer traffic for one or more service activity classifications to one or more proxy gateway/servers, the device routing, re-directing, or steering is accomplished by routing, re-directing, or steering the device traffic for one or more service usage classifications to a specific network destination or resource associated with the proxy gateway/server. In some embodiments, the routing, re-directing, or steering is accomplished using a secure tunnel through the network. In

IPR2025-01572
Apple EX1002 Page 160

some embodiments the routing, re-directing, or steering is accomplished with a VPN or APN tunnel.

[00406] In some embodiments, a network-based service charging policy system is used in conjunction with a user service agreement confirmation system, wherein the user agreement confirmation system provides confirmation that the user has agreed to access service usage terms that stipulate a first rate of access service usage accounting or charging when a SIM is detected in association with a device configuration that includes a service processor capability, and a second rate of access service usage accounting or charging when a SIM is detected in association with a device configuration that does not include a service processor capability. In some embodiments, if a user removes or tampers with a device configuration that includes a service processor capability, or if a user installs a SIM in a device that is not configured with a service processor capability, the user service usage billing conditions are changed. In some embodiments, depending on the device configuration (e.g., with or without a service processor capability), the user is billed at a different rate for "bulk" service usage, or is billed at a different rate for one or more classifications of service usage.

[00407] In some embodiments, a network-based service charging policy system is used in conjunction with a user service agreement confirmation system, wherein the user agreement confirmation system provides confirmation that the user has agreed to access service usage terms that stipulate a first set of access service privileges when a SIM is detected in association with a device configuration that includes a service processor capability, and a second set of access service privileges when a SIM is detected in association with a device configuration that does not include a service processor capability. In some embodiments, if a user removes or tampers with a device configuration that includes a service processor capability, or if a user installs a SIM in a device that is not configured with a service processor capability, the user service usage permissions are modified. In some embodiments, this modification can include altering the allowed network destinations, altering the allowed network services, altering the allowed network resources, quarantining access or blocking access.

IPR2025-01572
Apple EX1002 Page 161

[00408] In some embodiments the presence of a device service processor in combination with a SIM results in the service controller providing advantageous network access services to the user. Examples include but are not limited to the sponsored services discussed herein, user-paid application-based services (e.g., user-paid services where access for one or more device applications is included in a service allowance with potentially lower cost than overall internet access), user-paid destination services (e.g., user-paid services where access for one or more network destinations or resources is included in a service allowance with potentially lower cost than overall internet access), roaming services (e.g., services that aid the user when the device is connected to a roaming network, such as by informing the user that she is roaming and asking if she wishes to continue or block roaming service usage, up to date roaming service usage indication or cost indication, roaming service rate indications, allowing a user to decide which device service usage classifications he wishes to allow while roaming, etc.), or service usage notification services (e.g., providing the user with an update of how much service usage or cost has been incurred, informing the user of what service plans are available, informing the user when a service plan sign up may be advantageous to the user based on an activity or group of activities the user is attempting, or providing the user with a set of service plan sign up choices that can be selected and purchased in a device user interface (UI), etc.). In some embodiments, these user services are made possible by the capabilities of the service processor on the device in conjunction with a specific configuration of a service controller or other network elements on an access service provider network.

[00409] In some embodiments, if the SIM for a first network service provider is removed from the device and another SIM for a second network or service provider is installed, the user may not have access to the same services. In some embodiments, the service processor on the device detects that the SIM has been changed and informs the user through a device user interface (UI) notification that if the user changes SIMS or service provider networks, the user will lose certain services. In some embodiments, the services that will be lost are listed in a UI notification. In some embodiments the UI notification states that if the user wishes to regain access to certain services, the user can re-install the original SIM.

IPR2025-01572
Apple EX1002 Page 162

[00410] The above description is provided to enable any person skilled in the art to make and use the invention. Various modifications to the embodiments are possible, and the principles described herein may be applied to these and other embodiments and applications without departing from the spirit and scope of the invention. Thus, the invention is not intended to be limited to the embodiments and applications shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein.

[00411] 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.

[00412] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not of limitation. Likewise, the various diagrams may depict an example architectural or other configuration for the invention, which is done to aid in understanding the features and functionality that can be included in the invention. The invention is not restricted to the illustrated example architectures or configurations, but the desired features can be implemented using a variety of alternative architectures and configurations. Indeed, it will be apparent to one of skill in the art how alternative functional, logical or physical partitioning and configurations can be implemented to implement the desired features of the present invention. Also, a multitude of different

IPR2025-01572
Apple EX1002 Page 163

constituent module names other than those depicted herein can be applied to the various partitions. Additionally, with regard to flow diagrams, operational descriptions and method claims, the order in which the steps are presented herein shall not mandate that various embodiments be implemented to perform the recited functionality in the same order unless the context dictates otherwise.

[00413] Although the invention is described above in terms of various exemplary embodiments and implementations, it should be understood that the various features, aspects and functionality described in one or more of the individual embodiments are not limited in their applicability to the particular embodiment with which they are described, but instead can be applied, alone or in various combinations, to one or more of the other embodiments of the invention, whether or not such embodiments are described and whether or not such features are presented as being a part of a described embodiment. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments.

[00414] Terms and phrases used in this document, and variations thereof, unless otherwise expressly stated, should be construed as open ended as opposed to limiting. As examples of the foregoing: the term "including" should be read as meaning "including, without limitation" or the like; the term "example" is used to provide exemplary instances of the item in discussion, not an exhaustive or limiting list thereof; the terms "a" or "an" should be read as meaning "at least one," "one or more" or the like; and adjectives such as "conventional," "traditional," "normal," "standard," "known" and terms of similar meaning should not be construed as limiting the item described to a given time period or to an item available as of a given time, but instead should be read to encompass conventional, traditional, normal, or standard technologies that may be available or known now or at any time in the future. Likewise, where this document refers to technologies that would be apparent or known to one of ordinary skill in the art, such technologies encompass those apparent or known to the skilled artisan now or at any time in the future.

[00415] The presence of broadening words and phrases such as "one or more," "at

IPR2025-01572
Apple EX1002 Page 164

least," "but not limited to" or other like phrases in some instances shall not be read to mean that the narrower case is intended or required in instances where such broadening phrases may be absent. The use of the term "module" does not imply that the components or functionality described or claimed as part of the module are all configured in a common package. Indeed, any or all of the various components of a module, whether control logic or other components, can be combined in a single package or separately maintained and can further be distributed in multiple groupings or packages or across multiple locations.

[00416] Additionally, the various embodiments set forth herein are described in terms of exemplary block diagrams, flow charts and other illustrations. As will become apparent to one of ordinary skill in the art after reading this document, the illustrated embodiments and their various alternatives can be implemented without confinement to the illustrated examples. For example, block diagrams and their accompanying description should not be construed as mandating a particular architecture or configuration.

INCORPORATION BY REFERENCE

[00417] This document incorporates by reference for all purposes the following non-provisional U.S. patent applications: Application No. 12/380,778 (Attorney Docket No. RALEP004), filed March 2, 2009, entitled VERIFIABLE DEVICE ASSISTED SERVICE USAGE BILLING WITH INTEGRATED ACCOUNTING, MEDIATION ACCOUNTING, AND MULTI-ACCOUNT, now U.S. Patent No. 8,321,526 (issued November 27, 2012); Application No. 12/380,780 (Attorney Docket No. RALEP007), filed March 2, 2009, entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, now U.S. Patent No. 8,839,388 (issued September 16, 2014); Application No. 12/695,019 (Attorney Docket No. RALEP022), filed January 27, 2010, entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING, now U.S. Patent No. 8,275,830 (issued September 25, 2012); Application No. 12/695,020 (Attorney Docket No. RALEP024), filed January 27, 2010, entitled ADAPTIVE AMBIENT SERVICES, now U.S. Patent No. 8,406,748 (issued March 26,

IPR2025-01572
Apple EX1002 Page 165

2013); Application No. 12/694,445 (Attorney Docket No. RALEP025), filed January 27, 2010, entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES, now U.S. Patent No. 8,391,834 (issued March 5, 2013); Application No. 12/694,451 (Attorney Docket No. RALEP026), filed January 27, 2010, entitled DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM, now U.S. Patent No. 8,548,428 (issued October 1, 2013); Application No. 12/694,455 (Attorney Docket No. RALEP027), filed January 27, 2010, entitled DEVICE ASSISTED SERVICES INSTALL, now U.S. Patent No. 8,402,111 (issued March 19, 2013); Application No. 12/695,021 (Attorney Docket No. RALEP029), filed January 27, 2010, entitled QUALITY OF SERVICE FOR DEVICE ASSISTED SERVICES, now U.S. Patent No. 8,346,225 (issued January 1, 2013); Application No. 12/695,980 (Attorney Docket No. RALEP030), filed January 28, 2010, entitled ENHANCED ROAMING SERVICES AND CONVERGED CARRIER NETWORKS WITH DEVICE ASSISTED SERVICES AND A PROXY, now U.S. Patent No. 8,340,634 (issued December 25, 2012); Application No. 13/134,005 (Attorney Docket No. RALEP049), filed May 25, 2011, entitled SYSTEM AND METHOD FOR WIRELESS NETWORK OFFLOADING, now U.S. Patent No. 8,635,335 (issued January 21, 2014); Application No. 13/134,028 (Attorney Docket No. RALEP032), filed May 25, 2011, entitled DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY, now U.S. Patent No. 8,589,541 (issued November 19, 2013); Application No. 13/229,580 (Attorney Docket No. RALEP033), filed September 9, 2011, entitled WIRELESS NETWORK SERVICE INTERFACES, now U.S. Patent No. 8,626,115 (issued January 7, 2014); Application No. 13/237,827 (Attorney Docket No. RALEP034), filed September 20, 2011, entitled ADAPTING NETWORK POLICIES BASED ON DEVICE SERVICE PROCESSOR CONFIGURATION, now U.S. Patent No. 8,832,777 (issued September 9, 2014); Application No. 13/239,321 (Attorney Docket No. RALEP036), filed September 21, 2011, entitled SERVICE OFFER SET PUBLISHING TO DEVICE AGENT WITH ON-DEVICE SERVICE SELECTION, now U.S. Patent No. 8,898,293 (issued November 25, 2014); Application No. 13/248,028 (Attorney Docket No. RALEP037), filed September 28, 2011, entitled ENTERPRISE ACCESS CONTROL AND ACCOUNTING ALLOCATION FOR ACCESS NETWORKS, now U.S. Patent No. 8,924,469 (issued

IPR2025-01572
Apple EX1002 Page 166

December 30, 2014); Application No. 13/247,998 (Attorney Docket No. RALEP038), filed September 28, 2011, entitled COMMUNICATIONS DEVICE WITH SECURE DATA PATH PROCESSING AGENTS, now U.S. Patent No. 8,725,123 (issued May 13, 2014); Application No. 13/248,025 (Attorney Docket No. RALEP043), filed September 28, 2011, entitled SERVICE DESIGN CENTER FOR DEVICE ASSISTED SERVICES, now U.S. Patent No. 8,924,543 (issued December 30, 2014); Application No. 13/253,013 (Attorney Docket No. RALEP035), filed October 4, 2011, entitled SYSTEM AND METHOD FOR PROVIDING USER NOTIFICATIONS, now U.S. Patent No. 8,745,191 (issued June 3, 2014); Application No. 13/309,556 (Attorney Docket No. RALEP040), filed December 1, 2011, entitled END USER DEVICE THAT SECURES AN ASSOCIATION OF APPLICATION TO SERVICE POLICY WITH AN APPLICATION CERTIFICATE CHECK, now U.S. Patent No. 8,893,009 (issued November 18, 2014); and Application No. 13/309,463 (Attorney Docket No. RALEP041), FILED DECMEBER 1, 2011, entitled SECURITY, FRAUD DETECTION, AND FRAUD MITIGATION IN DEVICE-ASSISTED SERVICES SYSTEMS, now U.S. Patent No. 8,793,758 (issued July 29, 2014).

[00418] This document incorporates by reference for all purposes the following provisional patent applications: Provisional Application No. 61/206,354 (Attorney Docket No. RALEP001+), filed January 28, 2009, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD; Provisional Application No. 61/206,944 (Attorney Docket No. RALEP002+), filed February 4, 2009, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD; Provisional Application No. 61/207,393 (Attorney Docket No. RALEP003+), filed February 10, 2009, entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD; and Provisional Application No. 61/207,739 (Attorney Docket No. RALEP004+), entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD, filed February 13, 2009; Provisional Application No. 61/270,353 (Attorney Docket No. RALEP022+), filed on July 6, 2009, entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING; Provisional Application No. 61/275,208 (Attorney Docket No. RALEP023+), filed August 25, 2009, entitled ADAPTIVE AMBIENT SERVICES; and Provisional Application No. 61/237,753

IPR2025-01572
Apple EX1002 Page 167

(Attorney Docket No. RALEP024+), filed August 28, 2009, entitled ADAPTIVE AMBIENT SERVICES; Provisional Application No. 61/252,151 (Attorney Docket No. RALEP025+), filed October 15, 2009, entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES; Provisional Application No. 61/252,153 (Attorney Docket No. RALEP026+), filed October 15, 2009, entitled DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM; Provisional Application No. 61/264,120 (Attorney Docket No. RALEP027+), filed November 24, 2009, entitled DEVICE ASSISTED SERVICES INSTALL; Provisional Application No. 61/264,126 (Attorney Docket No. RALEP028+), filed November 24, 2009, entitled DEVICE ASSISTED SERVICES ACTIVITY MAP; Provisional Application No. 61/348,022 (Attorney Docket No. RALEP031+), filed May 25, 2010, entitled DEVICE ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY; Provisional Application No. 61/381,159 (Attorney Docket No. RALEP032+), filed September 9, 2010, entitled DEVICE ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY; Provisional Application No. 61/381,162 (Attorney Docket No. RALEP033+), filed September 9, 2010, entitled SERVICE CONTROLLER INTERFACES AND WORKFLOWS; Provisional Application No. 61/384,456 (Attorney Docket No. RALEP034+), filed September 20, 2010, entitled SECURING SERVICE PROCESSOR WITH SPONSORED SIMS; Provisional Application No. 61/389,547 (Attorney Docket No. RALEP035+), filed October 4, 2010, entitled USER NOTIFICATIONS FOR DEVICE ASSISTED SERVICES; Provisional Application No. 61/385,020 (Attorney Docket No. RALEP036+), filed September 21, 2010, entitled SERVICE USAGE RECONCILIATION SYSTEM OVERVIEW; Provisional Application No. 61/387,243 (Attorney Docket No. RALEP037+), filed September 28, 2010, entitled ENTERPRISE AND CONSUMER BILLING ALLOCATION FOR WIRELESS COMMUNICATION DEVICE SERVICE USAGE ACTIVITIES; Provisional Application No. 61/387,247 (Attorney Docket No. RALEP038+), filed September 28, entitled SECURED DEVICE DATA RECORDS, 2010; Provisional Application No. 61/407,358 (Attorney Docket No. RALEP039+), filed October 27, 2010, entitled SERVICE CONTROLLER AND SERVICE PROCESSOR ARCHITECTURE; Provisional Application No. 61/418,507 (Attorney Docket No. RALEP040+), filed December 1, 2010, entitled APPLICATION

IPR2025-01572
Apple EX1002 Page 168

SERVICE PROVIDER INTERFACE SYSTEM; Provisional Application No. 61/418,509 (Attorney Docket No. RALEP041+), filed December 1, 2010, entitled SERVICE USAGE REPORTING RECONCILIATION AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES; Provisional Application No. 61/420,727 (Attorney Docket No. RALEP042+), filed December 7, 2010, entitled SECURE DEVICE DATA RECORDS; Provisional Application No. 61/422,565 (Attorney Docket No. RALEP043+), filed December 13, 2010, entitled SERVICE DESIGN CENTER FOR DEVICE ASSISTED SERVICES; Provisional Application No. 61/422,572 (Attorney Docket No. RALEP044+), filed December 13, 2010, entitled SYSTEM INTERFACES AND WORKFLOWS FOR DEVICE ASSISTED SERVICES; Provisional Application No. 61/422,574 (Attorney Docket No. RALEP045+), filed December 13, 2010, entitled SECURITY AND FRAUD DETECTION FOR DEVICE ASSISTED SERVICES; Provisional Application No. 61/435,564 (Attorney Docket No. RALEP046+), filed January 24, 2011, entitled FRAMEWORK FOR DEVICE ASSISTED SERVICES; Provisional Application No. 61/472,606 (Attorney Docket No. RALEP047+), filed April 6, 2011, entitled MANAGING SERVICE USER DISCOVERY AND SERVICE LAUNCH OBJECT PLACEMENT ON A DEVICE; Provisional Application No. 61/550,906 (Attorney Docket No. RALEP048+), filed October 24, 2011, entitled SECURITY FOR DEVICE-ASSISTED SERVICES.

CLAIMS

1. An end-user device, comprising:

one or more modems for enabling the wireless end-user device to communicate over at least a first wireless access network;

memory configured to store

a first application program configured to execute on the wireless end-user device and further configured to assist the end-user device in accessing one or more data services over at least the first wireless access network,

a first application credential associated with the first application program,

a first policy comprising one or more first policy instructions to be applied when the first application program initiates or attempts to initiate a communication over the first wireless access network; and

one or more device agents configured to

detect an attempted installation of update software on the end-user device, the update software purporting to be a modification, update, or replacement of the first application program,

obtain an update-software credential associated with the update software,

obtain the first application credential,

allow the update software to be installed on the wireless end-user device if the update-software credential matches the first application credential,

determine when the first application program initiates or attempts to initiate a communication over the first wireless access network, and

apply the first policy when the first application program initiates or attempts to initiate a communication over the first wireless access network.

IPR2025-01572
Apple EX1002 Page 170

ABSTRACT

Secure architectures and methods for improving the security of mobile devices are disclosed. Also disclosed are apparatuses and methods to detect and mitigate fraud in device-assisted services implementations.

IPR2025-01572
Apple EX1002 Page 171

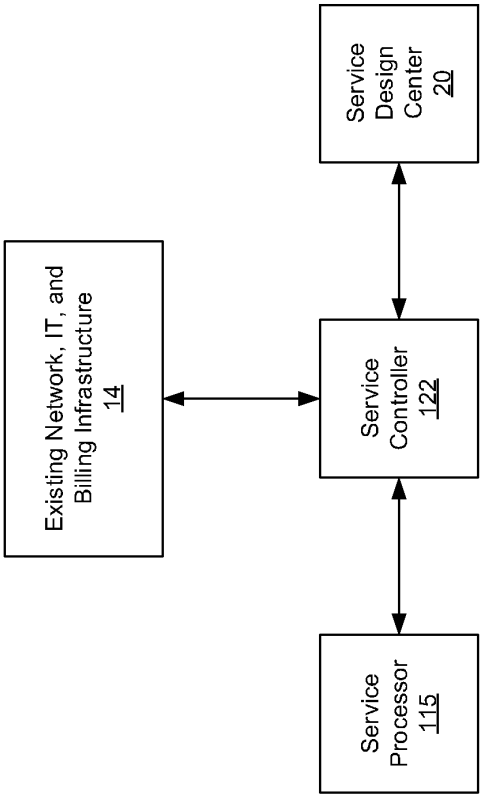

Service Design Center 20
Existing Network, IT, and Billing Infrastructure 14
Service Controller 122
Service Processor 115

FIG. 1

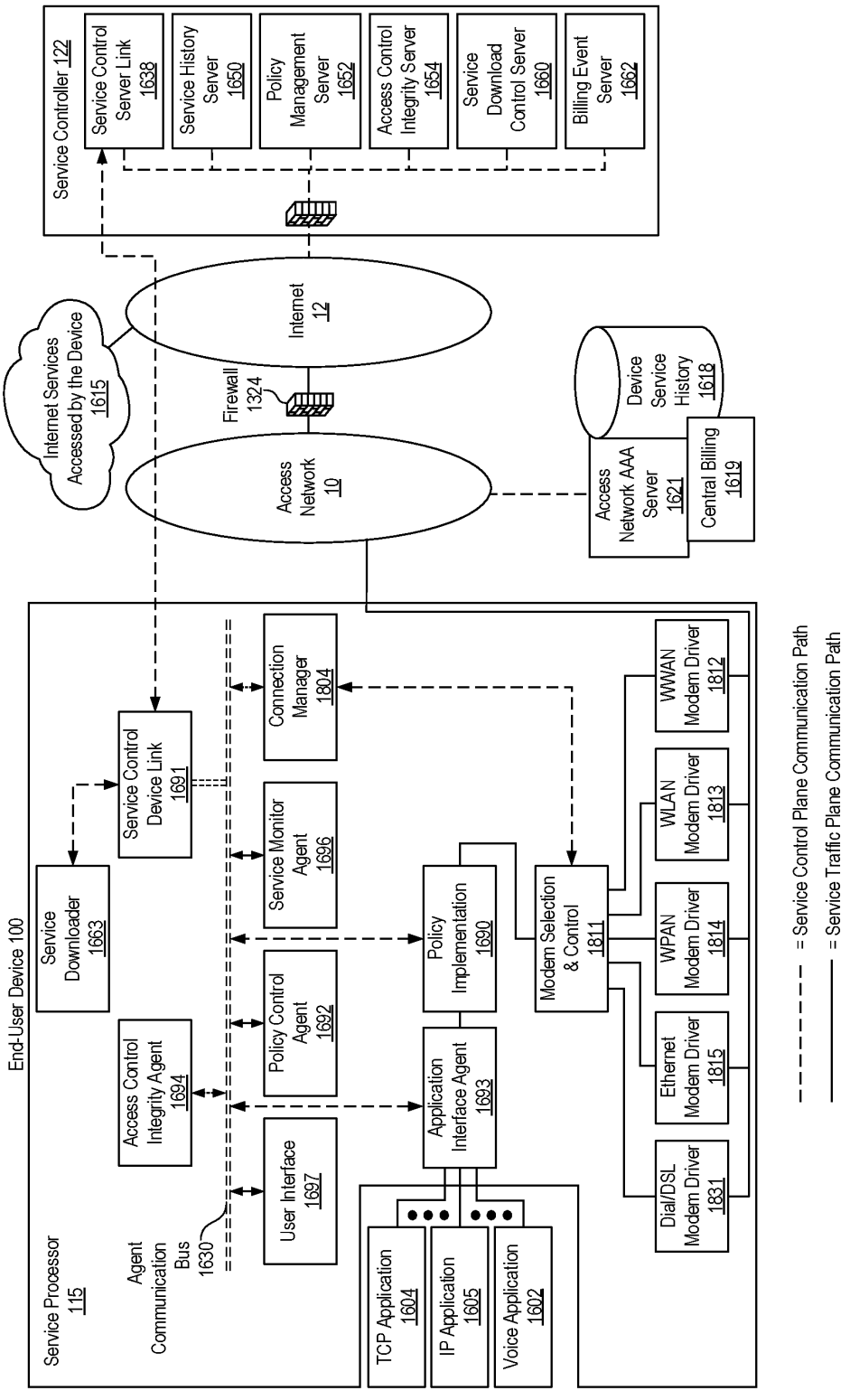

Service Controller 122
Service Control Server Link 1638
Service History Server 1650
Policy Management Server 1652
Access Control Integrity Server 1654
Service Download Control Server 1660
Billing Event Server 1662
Internet 12
Internet Services Accessed by the Device 1615
Firewall 1324
Access Network 10
Device Service History 1618
Access Network AAA Server 1621
Central Billing 1619
End-User Device 100
Service Processor 115
Agent Communication Bus 1630
Service Downloader 1663
Service Control Device Link 1691
Connection Manager 1804
Service Monitor Agent 1696
Access Control Integrity Agent 1694
Policy Control Agent 1692
Policy Implementation 1690
Modem Selection & Control 1811
User Interface 1697
Application Interface Agent 1693
WWAN Modem Driver 1812
WLAN Modem Driver 1813
WPAN Modem Driver 1814
Ethernet Modem Driver 1815
Dial/DSL Modem Driver 1831
TCP Application 1604
IP Application 1605
Voice Application 1602
= Service Control Plane Communication Path
= Service Traffic Plane Communication Path

FIG. 2

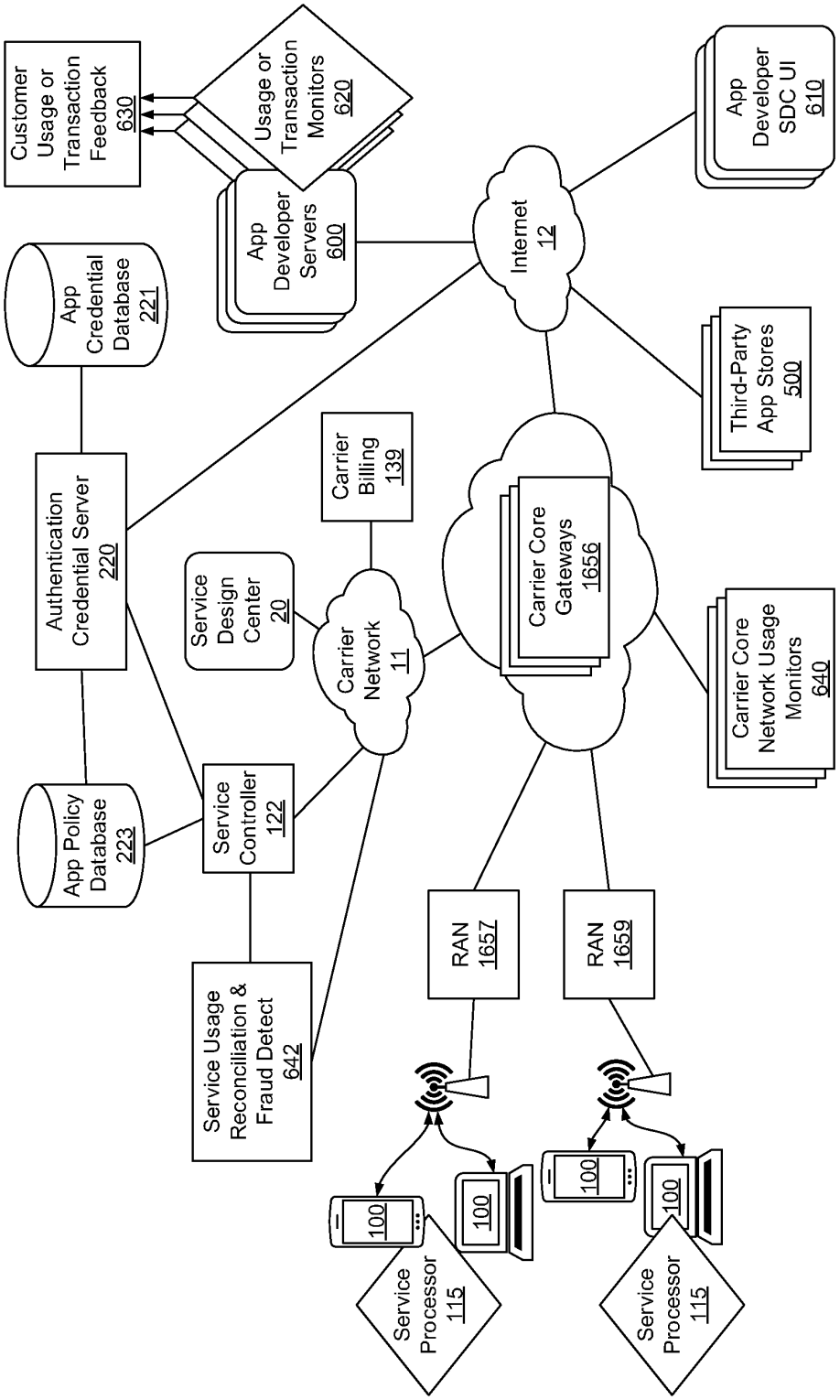

Customer Usage or Transaction Feedback 630
Usage or Transaction Monitors 620
App Developer Servers 600
Internet 12
App Developer SDC UI 610
App Credential Database 221
Third-Party App Stores 500
Authentication Credential Server 220
Carrier Billing 139
Service Design Center 20
Carrier Network 11
Carrier Core Gateways 1656
Carrier Core Network Usage Monitors 640
App Policy Database 223
Service Controller 122
Service Usage Reconciliation & Fraud Detect 642
RAN 1657
RAN 1659
100
100
100
100
Service Processor 115
Service Processor 115

FIG. 3

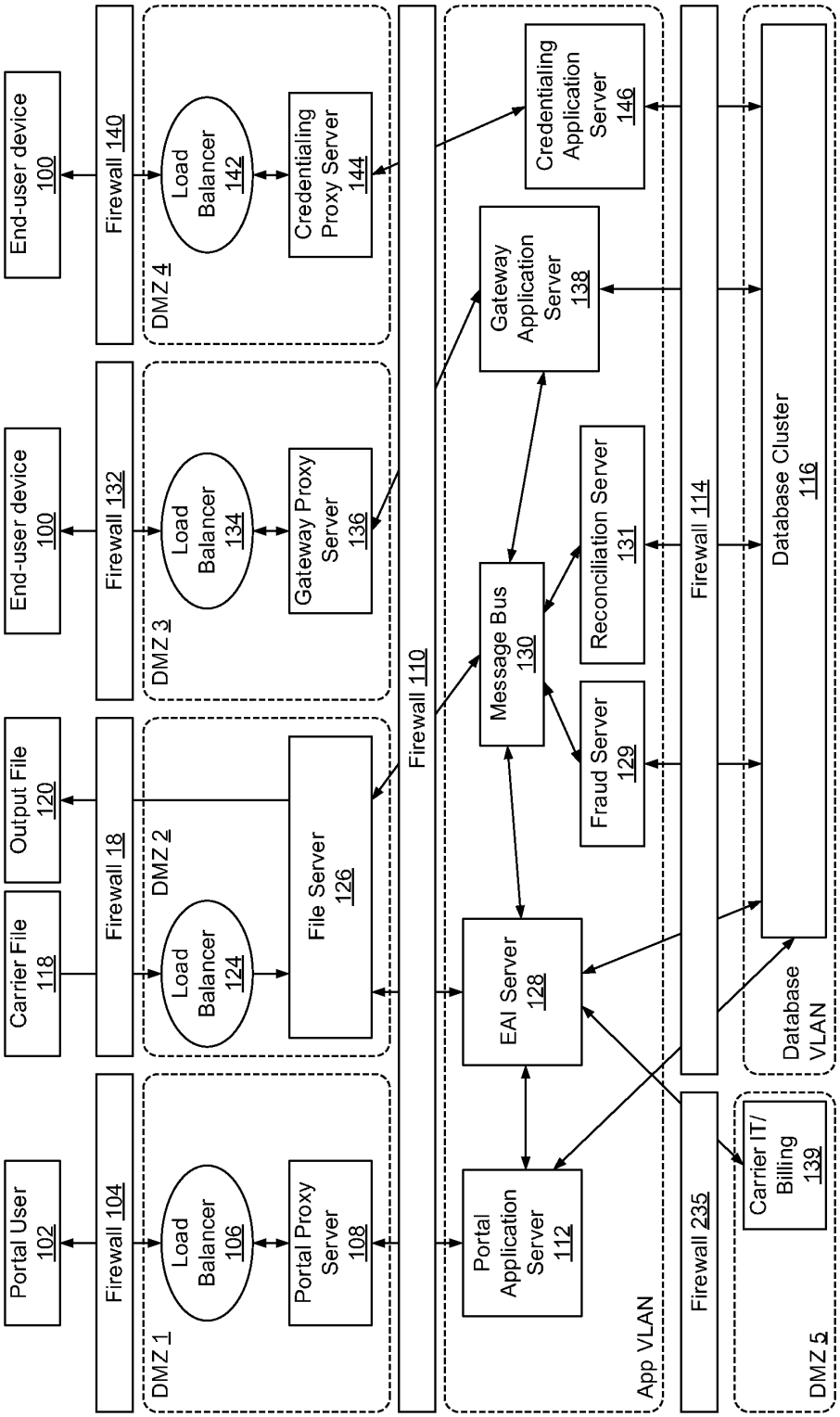

Portal User 102
End-user device 100
End-user device 100
Carrier File 118
Output File 120
Firewall 104
Firewall 18
Firewall 132
Firewall 140
DMZ 1
Load Balancer 106
Portal Proxy Server 108
DMZ 2
Load Balancer 124
File Server 126
DMZ 3
Load Balancer 134
Gateway Proxy Server 136
DMZ 4
Load Balancer 142
Credentialing Proxy Server 144
Firewall 110
App VLAN
Portal Application Server 112
EAI Server 128
Message Bus 130
Fraud Server 129
Reconciliation Server 131
Gateway Application Server 138
Credentialing Application Server 146
Firewall 114
Firewall 235
DMZ 5
Carrier IT/ Billing 139
Database VLAN
Database Cluster 116

FIG. 4

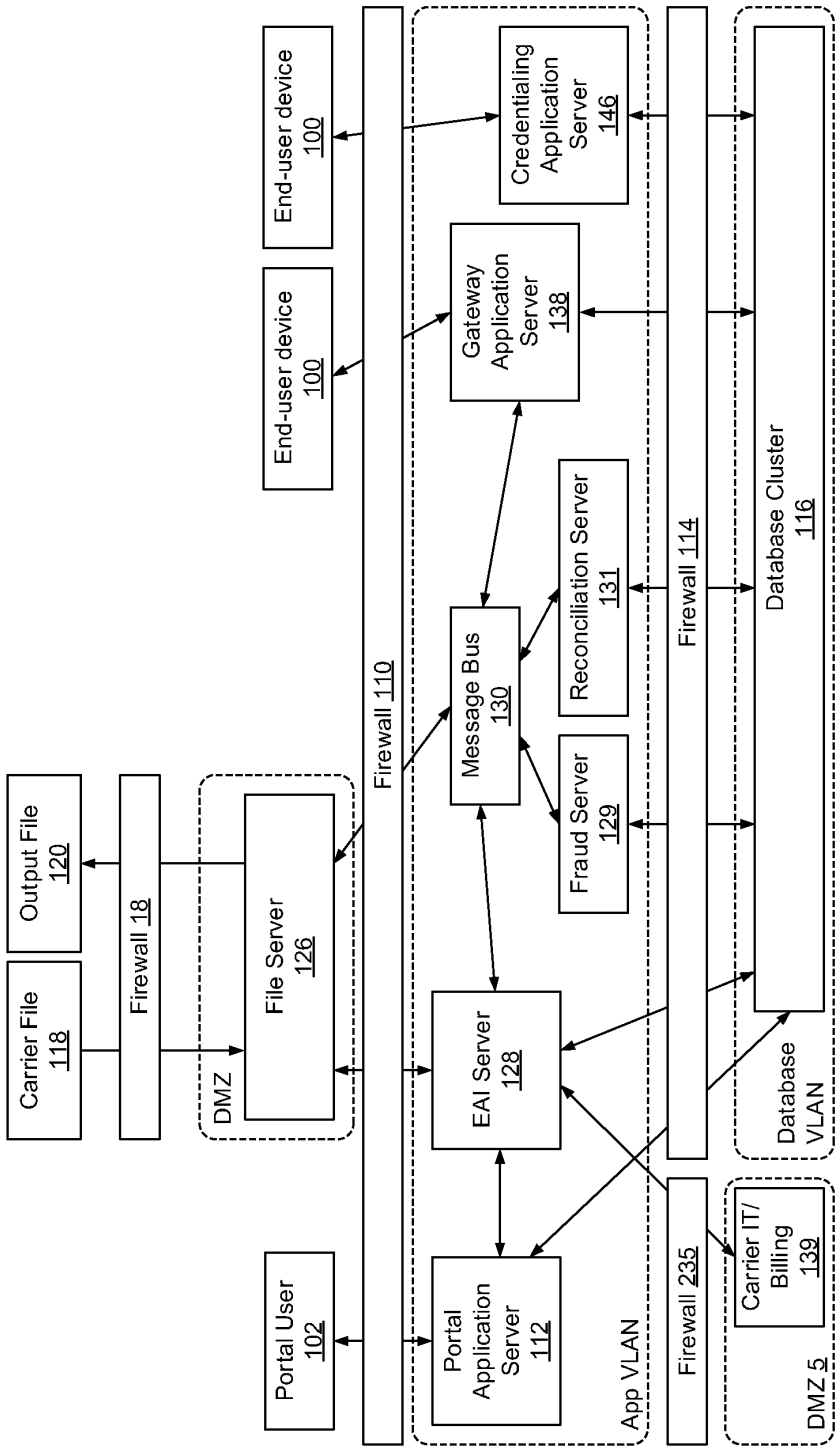

Output File 120
Carrier File 118
Firewall 18
DMZ
File Server 126
Firewall 110
End-user device 100
End-user device 100
Credentialing Application Server 146
Gateway Application Server 138
Message Bus 130
Reconciliation Server 131
Fraud Server 129
EAI Server 128
Portal User 102
Portal Application Server 112
App VLAN
Firewall 114
Database Cluster 116
Database VLAN
Firewall 235
Carrier IT/ Billing 139
DMZ 5

FIG. 5

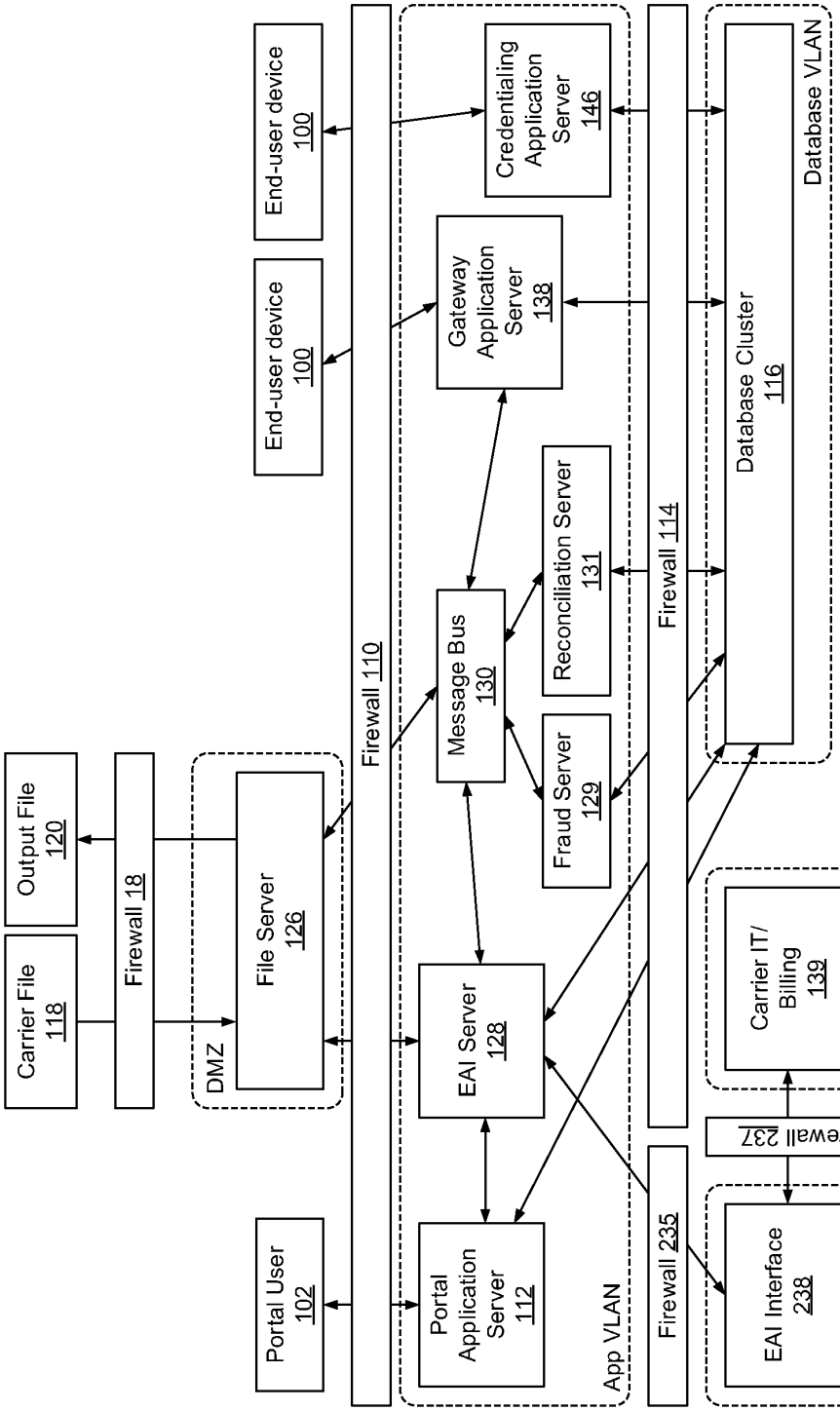

Carrier File 118
Output File 120
Firewall 18
DMZ
File Server 126
Portal User 102
Firewall 110
App VLAN
Portal Application Server 112
EAI Server 128
Message Bus 130
Fraud Server 129
Reconciliation Server 131
Gateway Application Server 138
Credentialing Application Server 146
End-user device 100
End-user device 100
Firewall 114
Firewall 235
Database VLAN
Database Cluster 116
Carrier IT/ Billing 139
DMZ 5
Firewall 237
EAI Interface 238
DMZ 6

FIG. 6

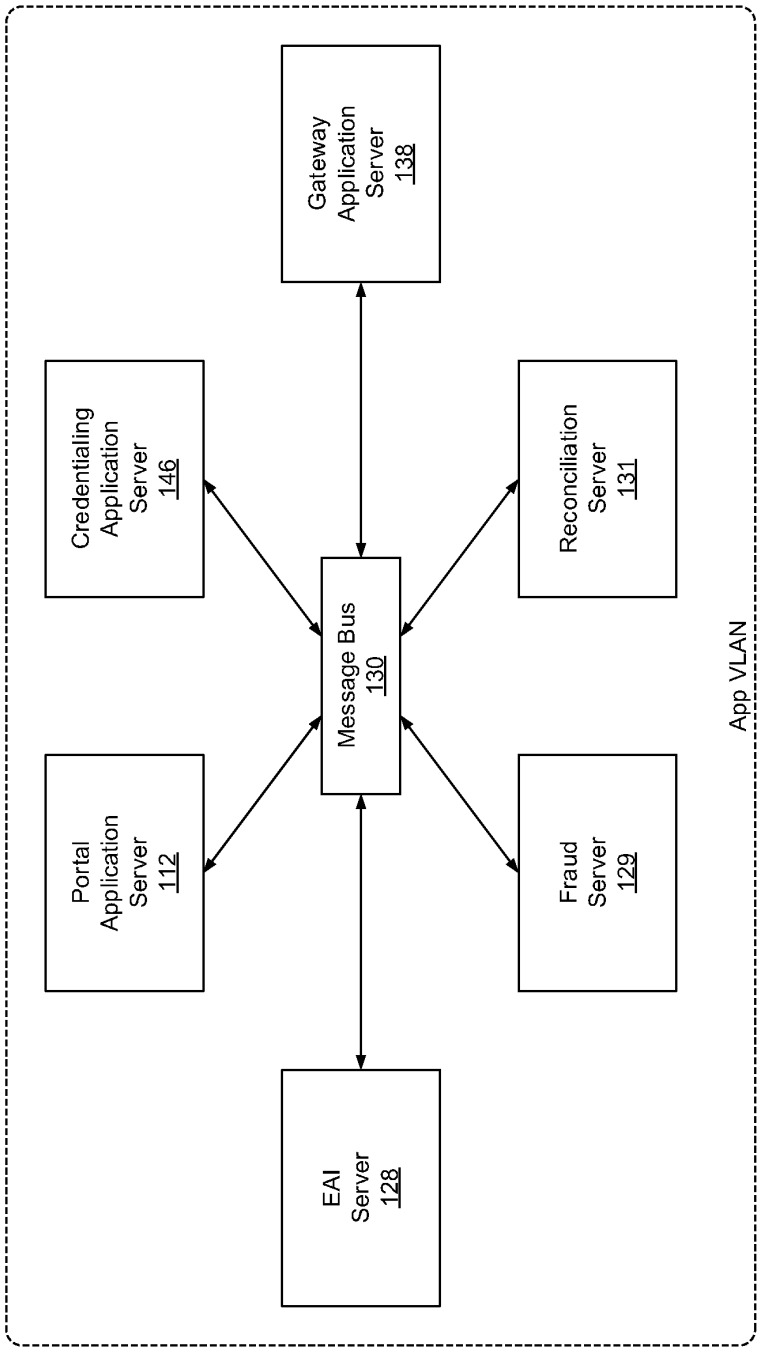

Gateway Application Server 138
Credentialing Application Server 146
Reconciliation Server 131
Message Bus 130
Portal Application Server 112
Fraud Server 129
EAI Server 128
App VLAN

FIG. 7

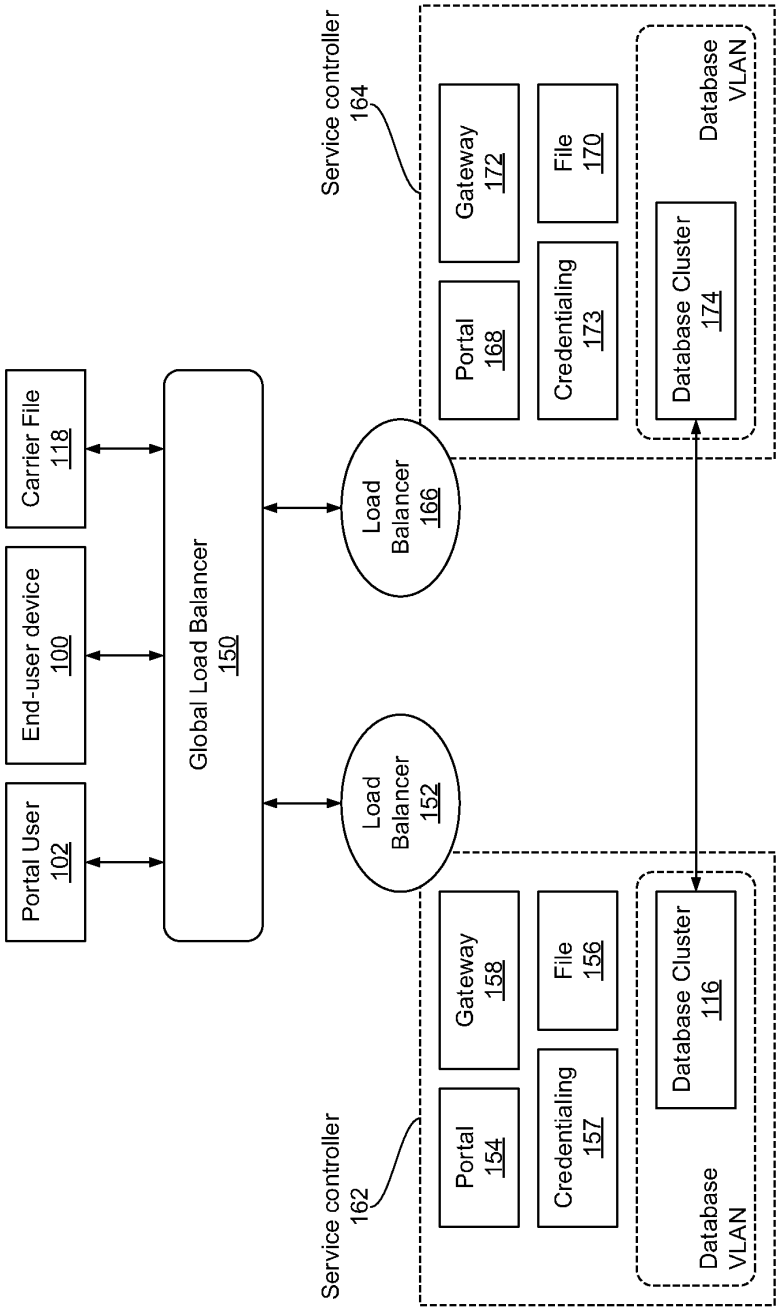

Portal User 102
End-user device 100
Carrier File 118
Global Load Balancer 150
Load Balancer 152
Load Balancer 166
Service controller 162
Portal 154
Gateway 158
Credentialing 157
File 156
Database Cluster 116
Database VLAN
Service controller 164
Portal 168
Gateway 172
Credentialing 173
File 170
Database Cluster 174
Database VLAN

FIG. 8

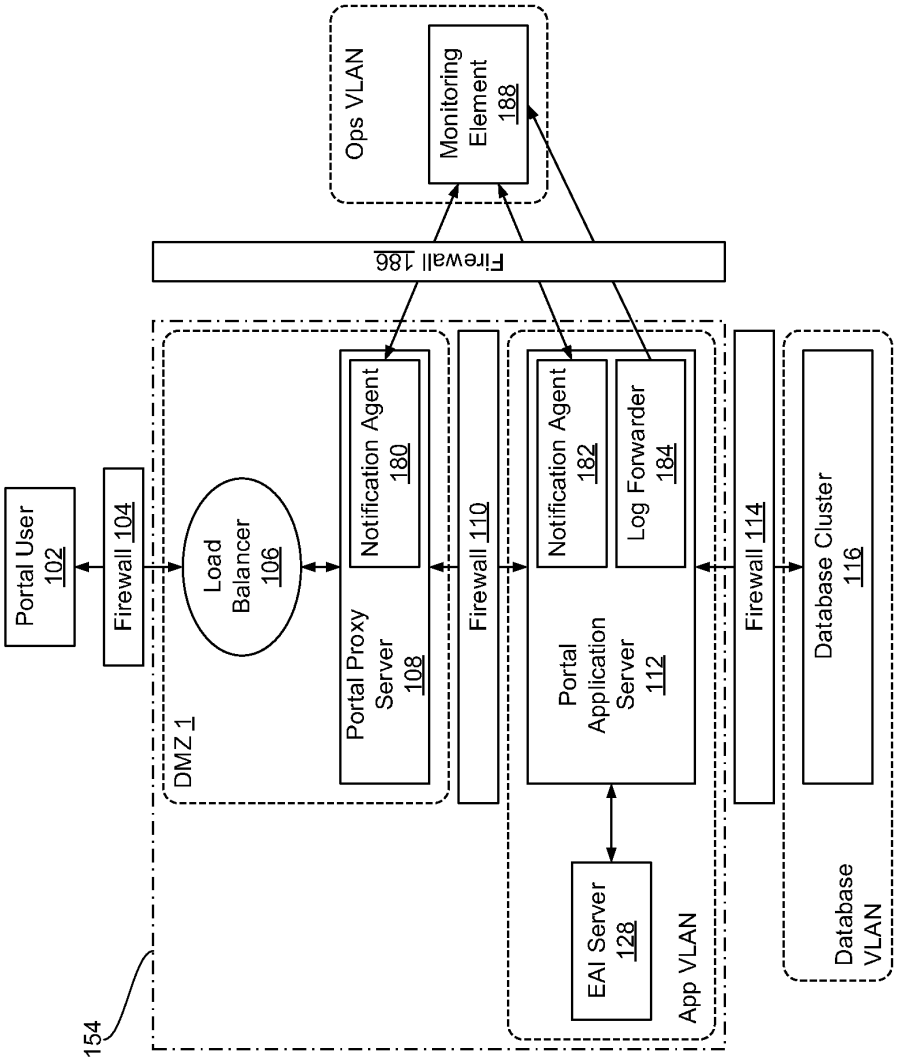

Ops VLAN
Monitoring Element 188
Firewall 186
Portal User 102
Firewall 104
Load Balancer 106
DMZ 1
Notification Agent 180
Portal Proxy Server 108
Firewall 110
Notification Agent 182
Log Forwarder 184
Portal Application Server 112
Firewall 114
Database Cluster 116
EAI Server 128
App VLAN
Database VLAN
154

FIG. 9

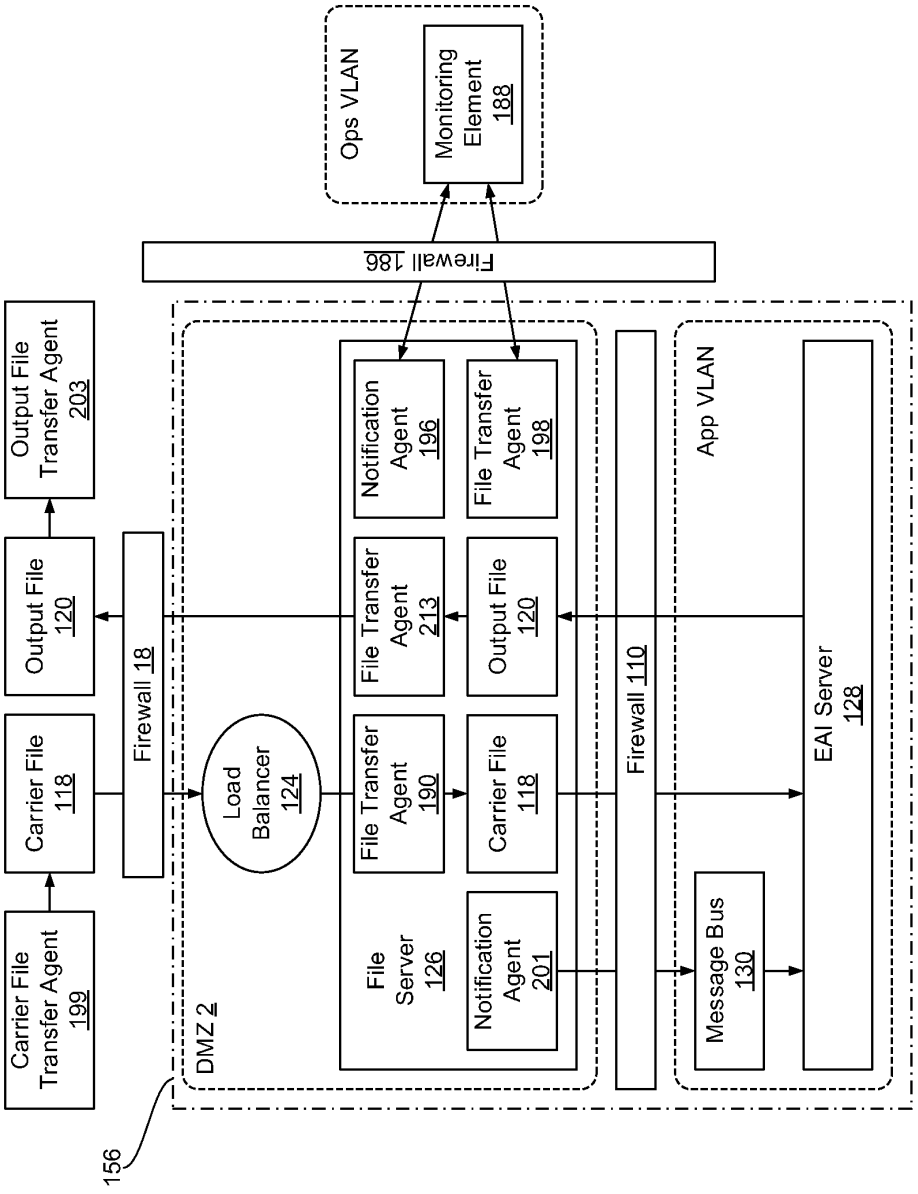

Ops VLAN
Monitoring Element 188
Firewall 186
Output File Transfer Agent 203
Output File 120
Firewall 18
Carrier File 118
Carrier File Transfer Agent 199
156
DMZ 2
Load Balancer 124
File Server 126
Notification Agent 196
File Transfer Agent 198
File Transfer Agent 213
Output File 120
File Transfer Agent 190
Carrier File 118
Notification Agent 201
Firewall 110
App VLAN
Message Bus 130
EAI Server 128

FIG. 10

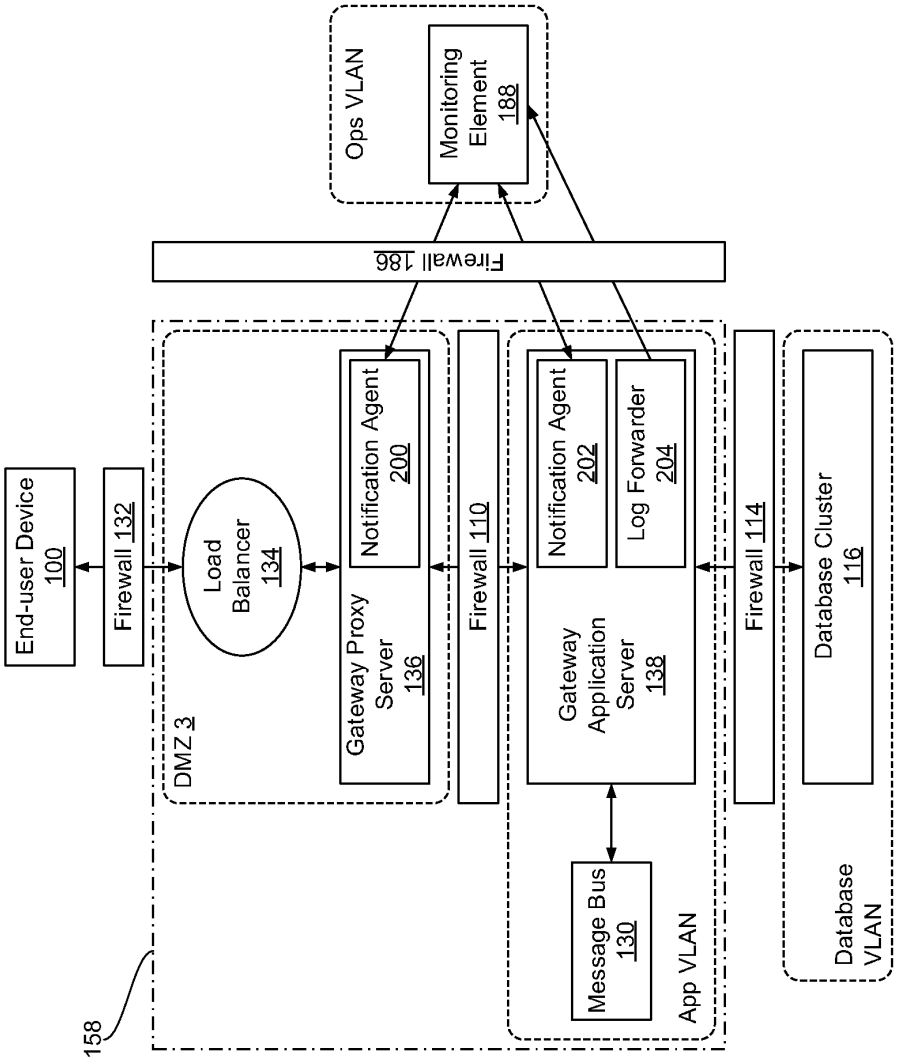

Ops VLAN
Monitoring Element 188
Firewall 186
End-user Device 100
Firewall 132
Load Balancer 134
DMZ 3
Notification Agent 200
Gateway Proxy Server 136
Firewall 110
Notification Agent 202
Log Forwarder 204
Gateway Application Server 138
Message Bus 130
App VLAN
Firewall 114
Database Cluster 116
Database VLAN
158

FIG. 11

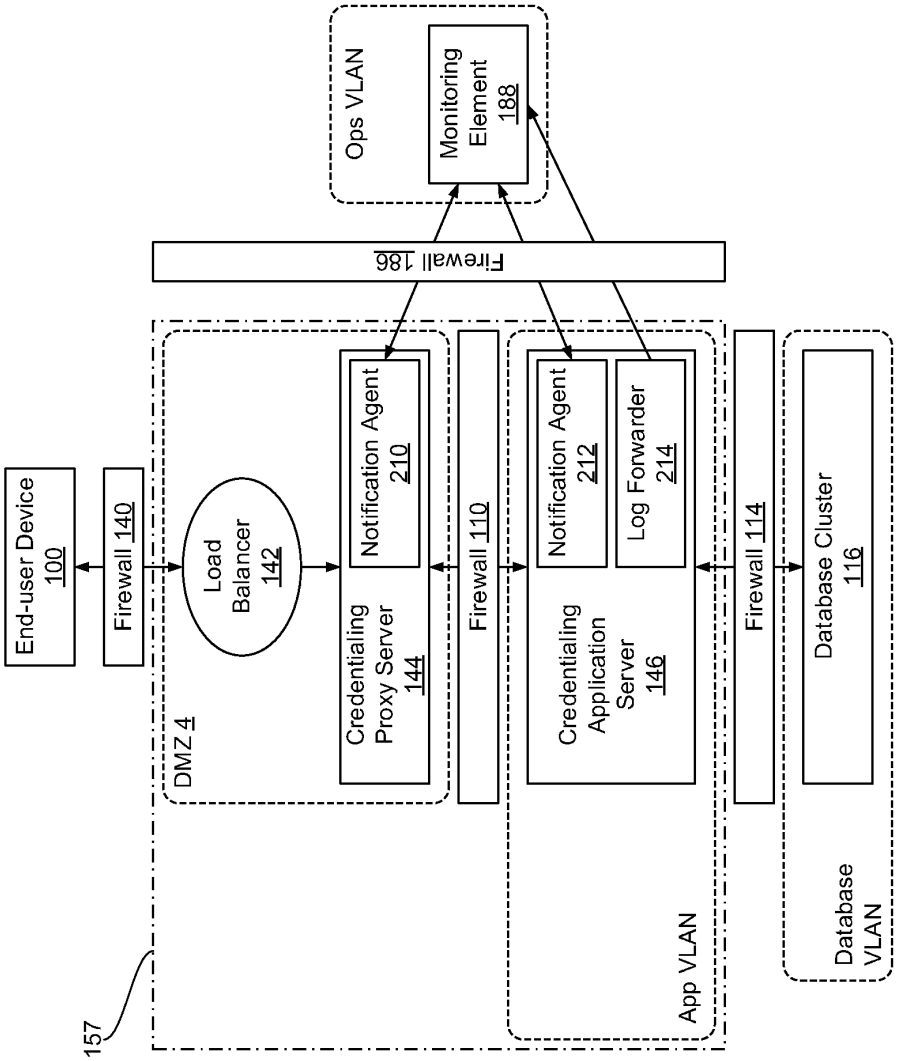

Ops VLAN
Monitoring Element 188
Firewall 186
End-user Device 100
Firewall 140
Load Balancer 142
DMZ 4
Notification Agent 210
Credentialing Proxy Server 144
Firewall 110
Notification Agent 212
Log Forwarder 214
Credentialing Application Server 146
App VLAN
Firewall 114
Database Cluster 116
Database VLAN
157

FIG. 12

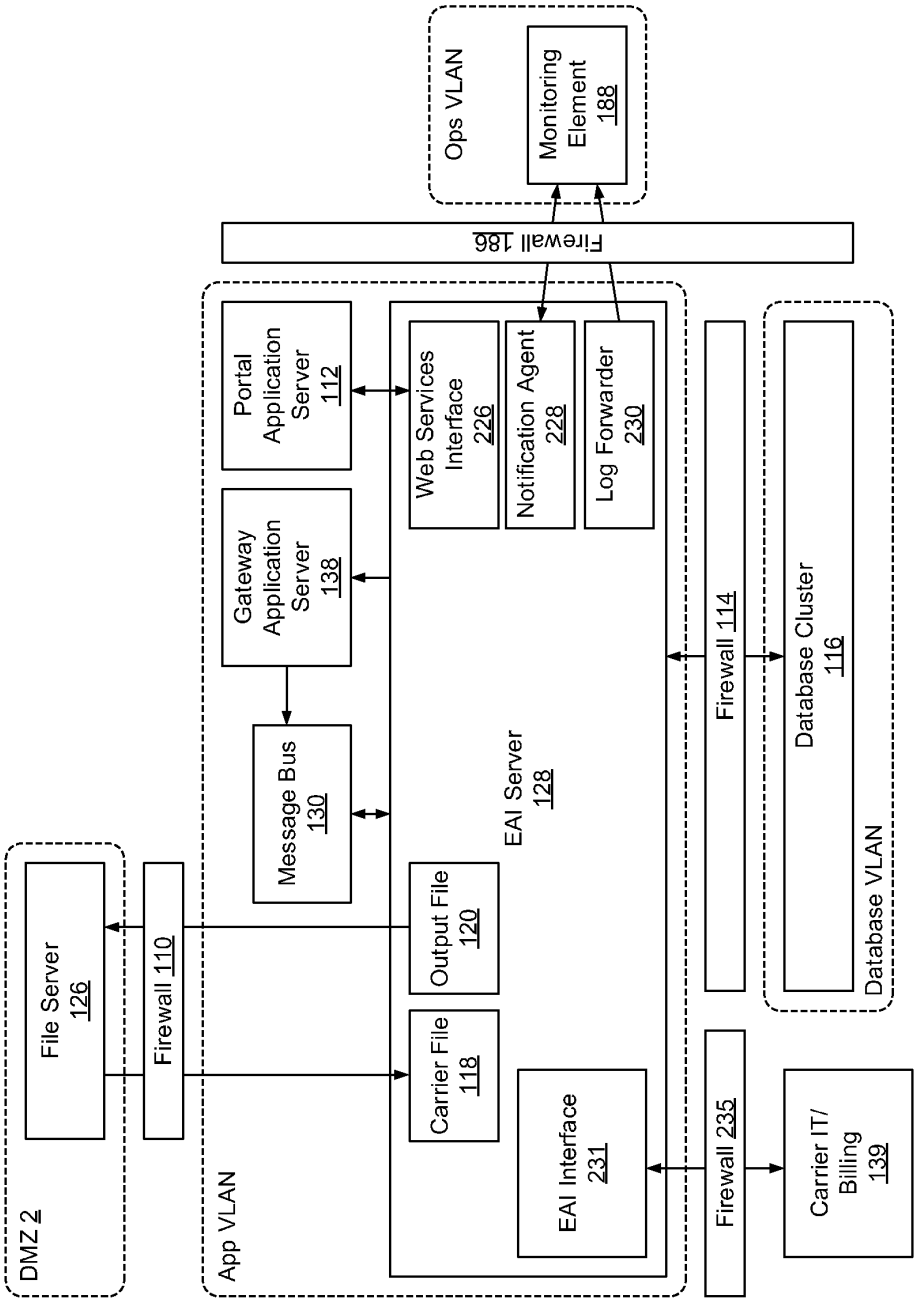

Ops VLAN
Monitoring Element 188
Firewall 186
Portal Application Server 112
Gateway Application Server 138
Message Bus 130
Web Services Interface 226
Notification Agent 228
Log Forwarder 230
EAI Server 128
Output File 120
Carrier File 118
EAI Interface 231
App VLAN
DMZ 2
File Server 126
Firewall 110
Firewall 114
Database Cluster 116
Database VLAN
Firewall 235
Carrier IT/ Billing 139

FIG. 13

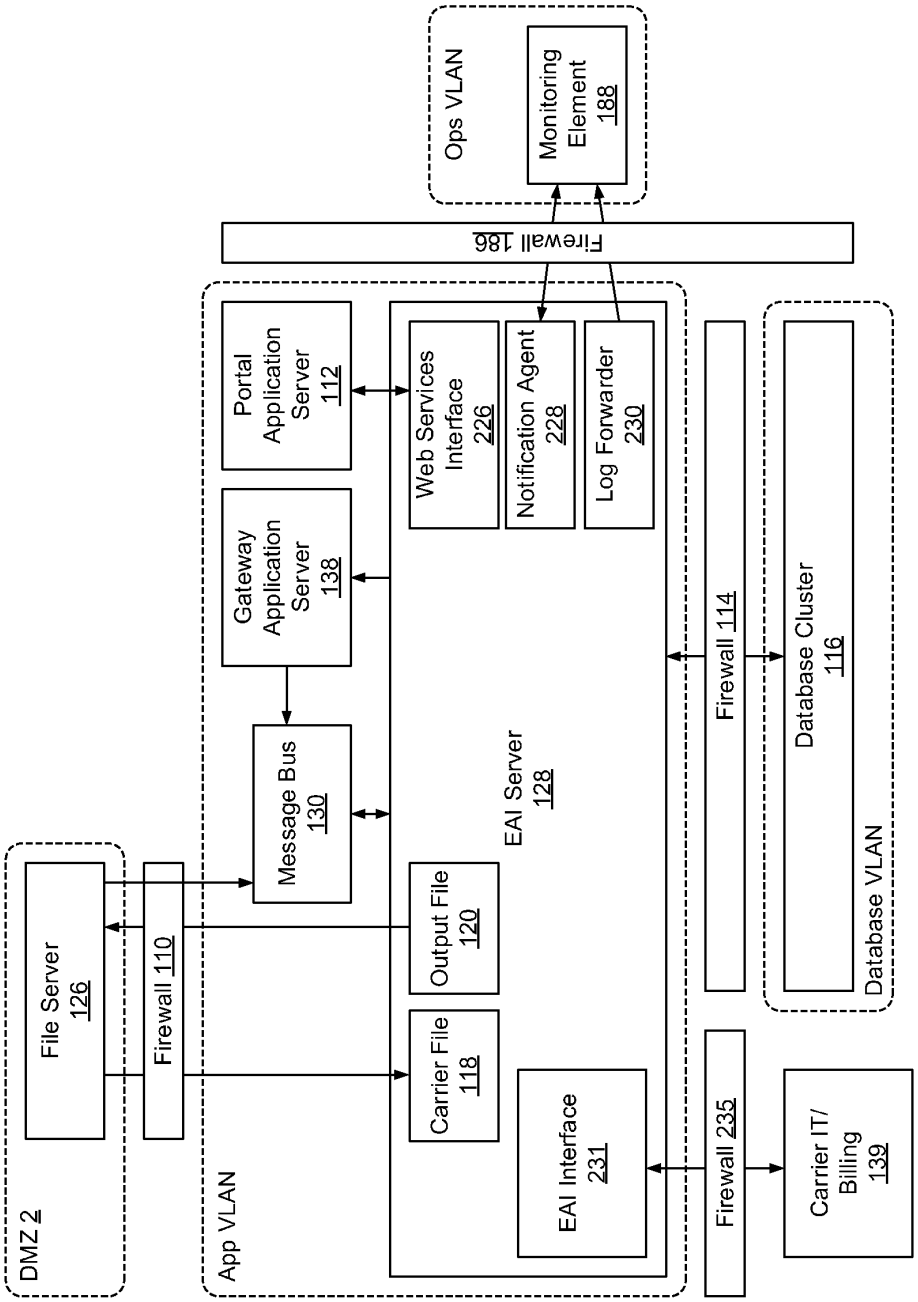

Ops VLAN
Monitoring Element 188
Firewall 186
Portal Application Server 112
Gateway Application Server 138
Message Bus 130
Web Services Interface 226
Notification Agent 228
Log Forwarder 230
EAI Server 128
Output File 120
Carrier File 118
EAI Interface 231
App VLAN
DMZ 2
File Server 126
Firewall 110
Firewall 114
Database Cluster 116
Database VLAN
Firewall 235
Carrier IT/ Billing 139

FIG. 14

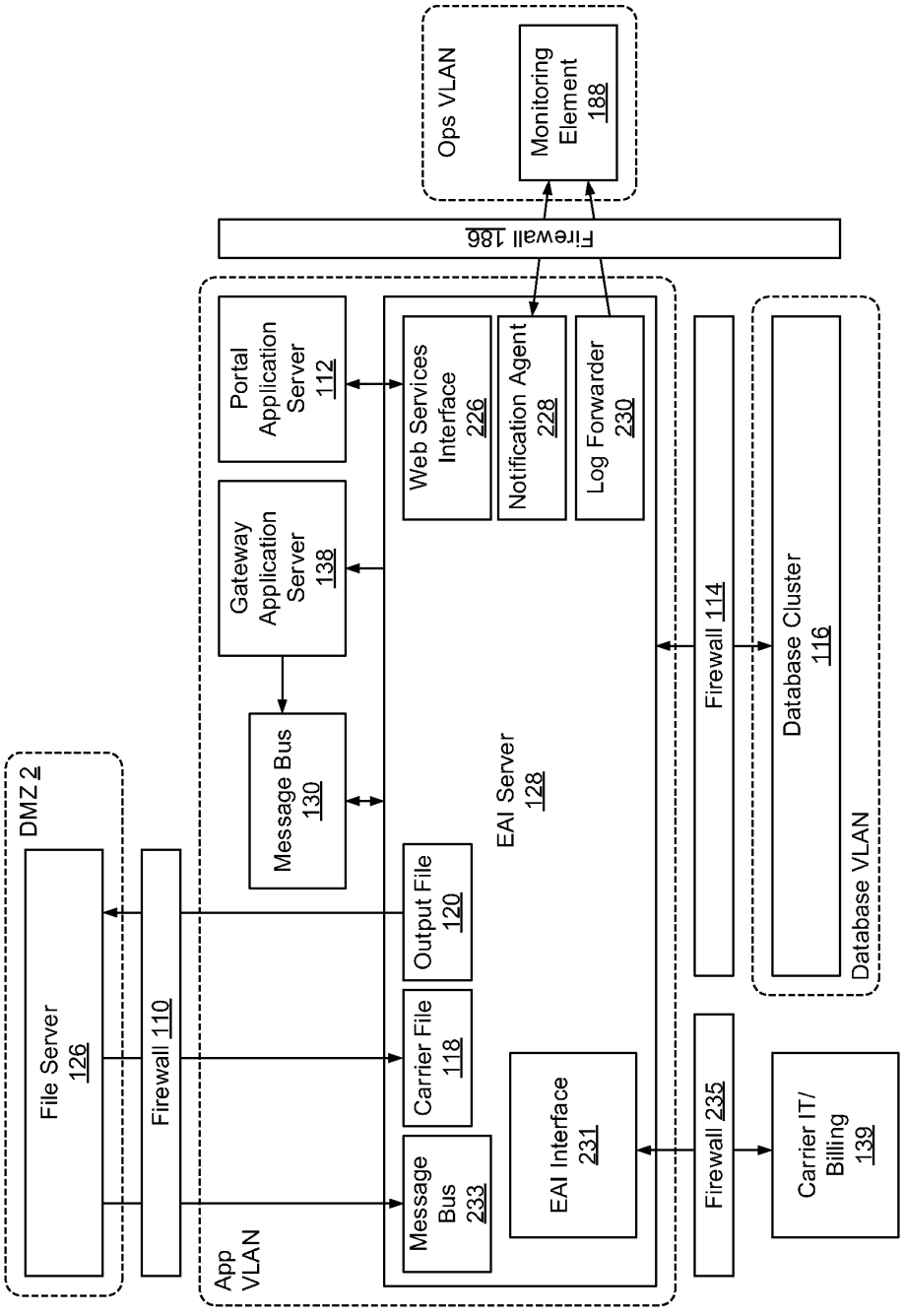

Ops VLAN
Monitoring Element 188
Firewall 186
Portal Application Server 112
Gateway Application Server 138
Message Bus 130
Web Services Interface 226
Notification Agent 228
Log Forwarder 230
EAI Server 128
Output File 120
Carrier File 118
Message Bus 233
EAI Interface 231
App VLAN
DMZ 2
File Server 126
Firewall 110
Firewall 114
Database Cluster 116
Database VLAN
Firewall 235
Carrier IT/ Billing 139

FIG. 15

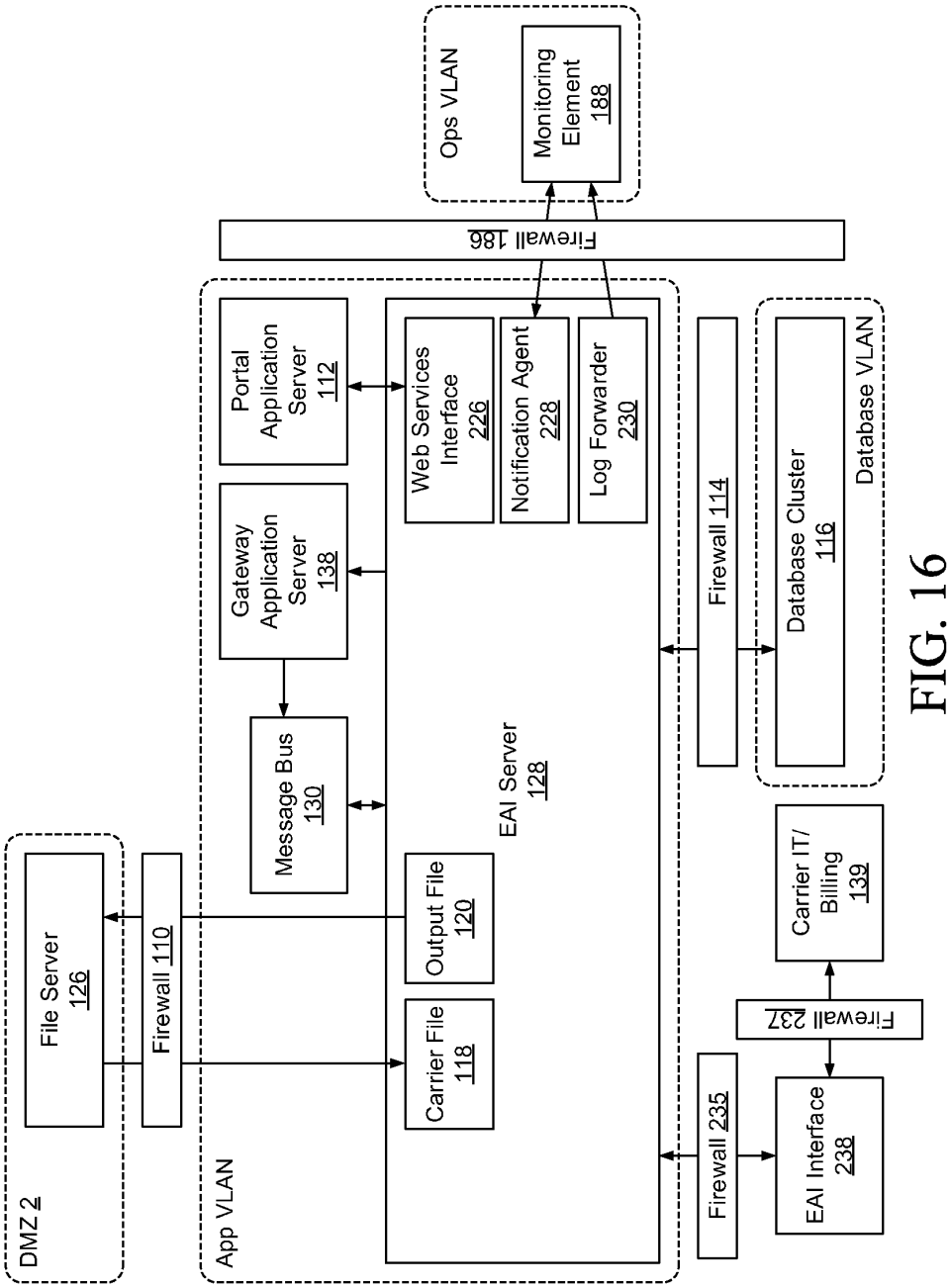

Ops VLAN
Monitoring Element 188
Firewall 186
Portal Application Server 112
Web Services Interface 226
Notification Agent 228
Log Forwarder 230
Gateway Application Server 138
Message Bus 130
EAI Server 128
Output File 120
Carrier File 118
Firewall 114
Database Cluster 116
Database VLAN
Carrier IT/ Billing 139
Firewall 237
EAI Interface 238
Firewall 235
File Server 126
Firewall 110
DMZ 2
App VLAN

FIG. 16

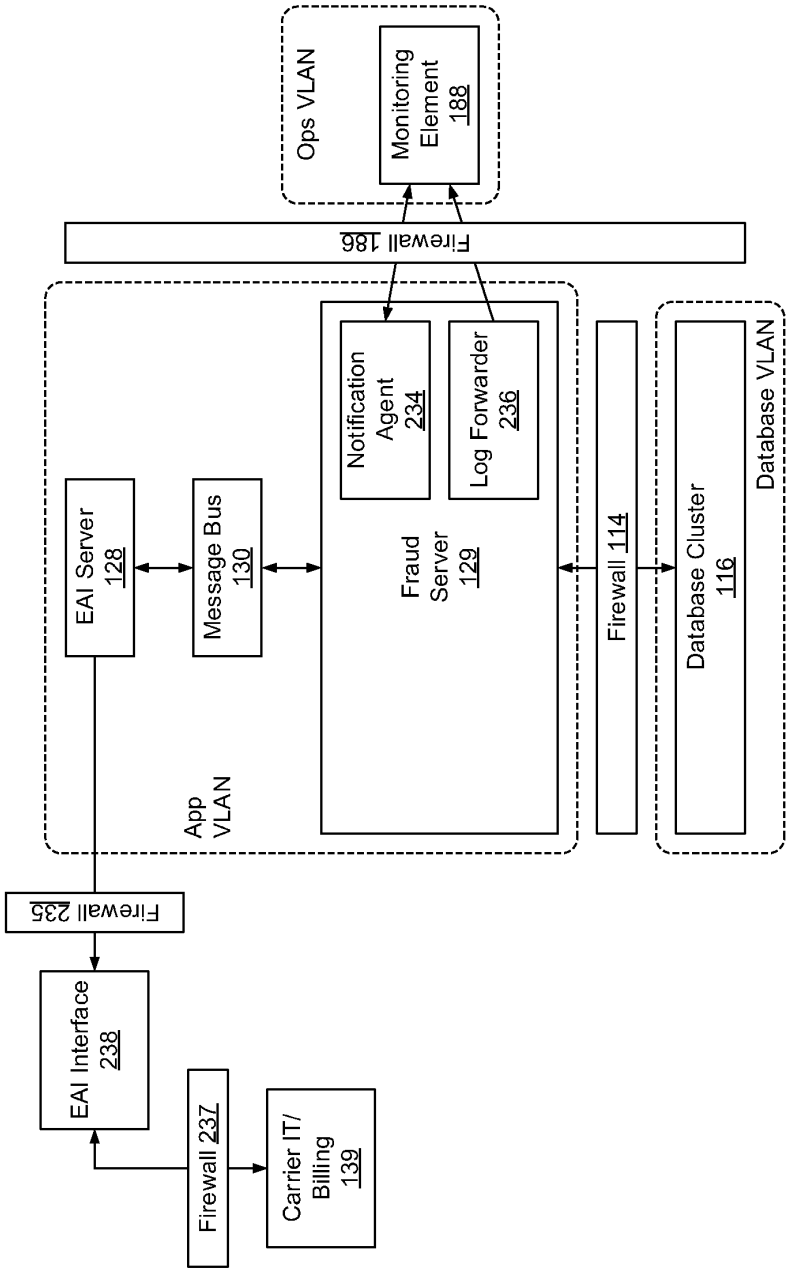

Ops VLAN
Monitoring Element 188
Firewall 186
Notification Agent 234
Log Forwarder 236
EAI Server 128
Message Bus 130
Fraud Server 129
Firewall 114
Database Cluster 116
Database VLAN
App VLAN
Firewall 235
EAI Interface 238
Firewall 237
Carrier IT/ Billing 139

FIG. 17

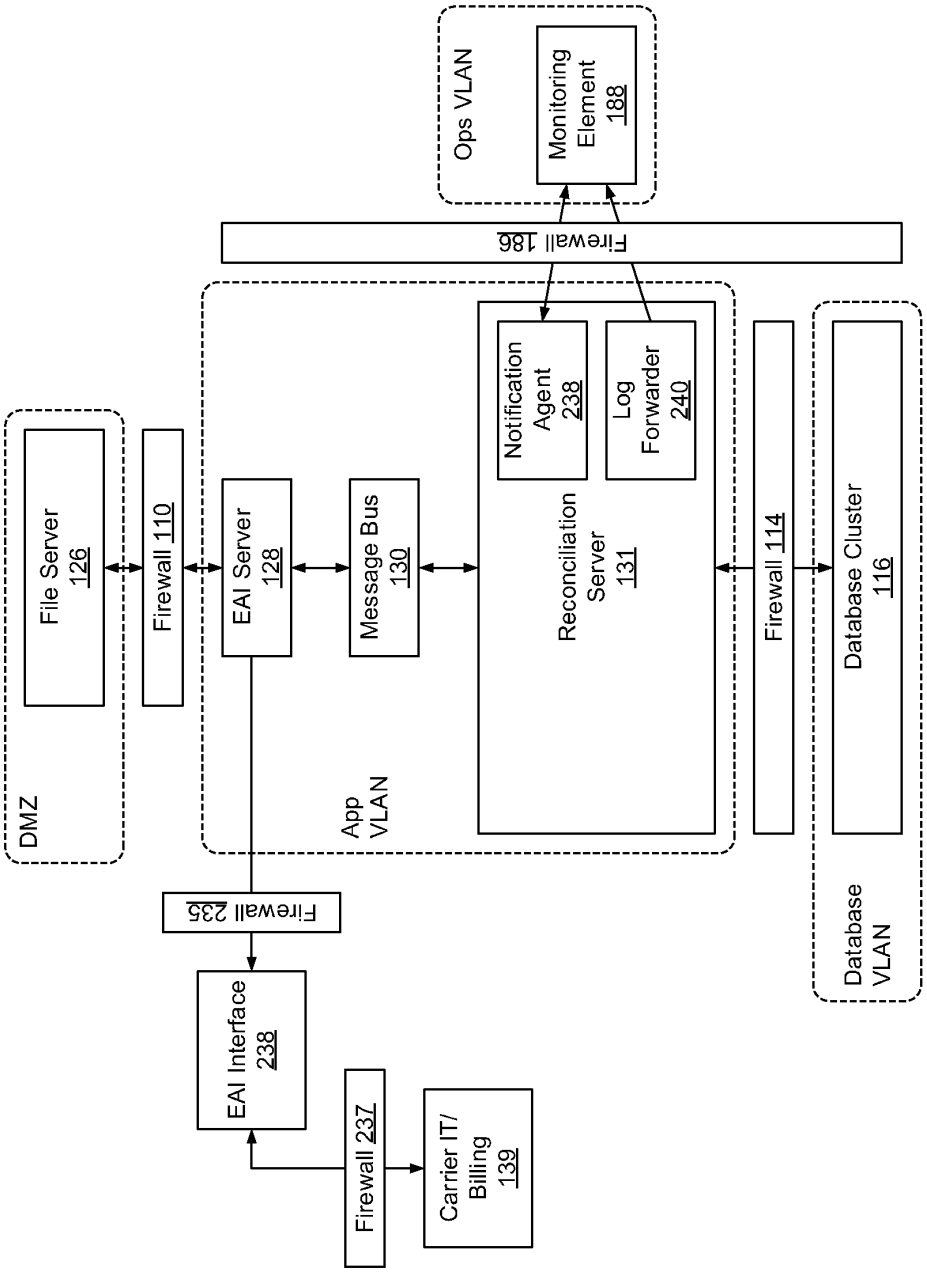

Ops VLAN
Monitoring Element 188
Firewall 186
Notification Agent 238
Log Forwarder 240
Reconciliation Server 131
Message Bus 130
EAI Server 128
Firewall 110
File Server 126
DMZ
App VLAN
Firewall 114
Database Cluster 116
Database VLAN
Firewall 235
EAI Interface 238
Firewall 237
Carrier IT/ Billing 139

FIG. 18

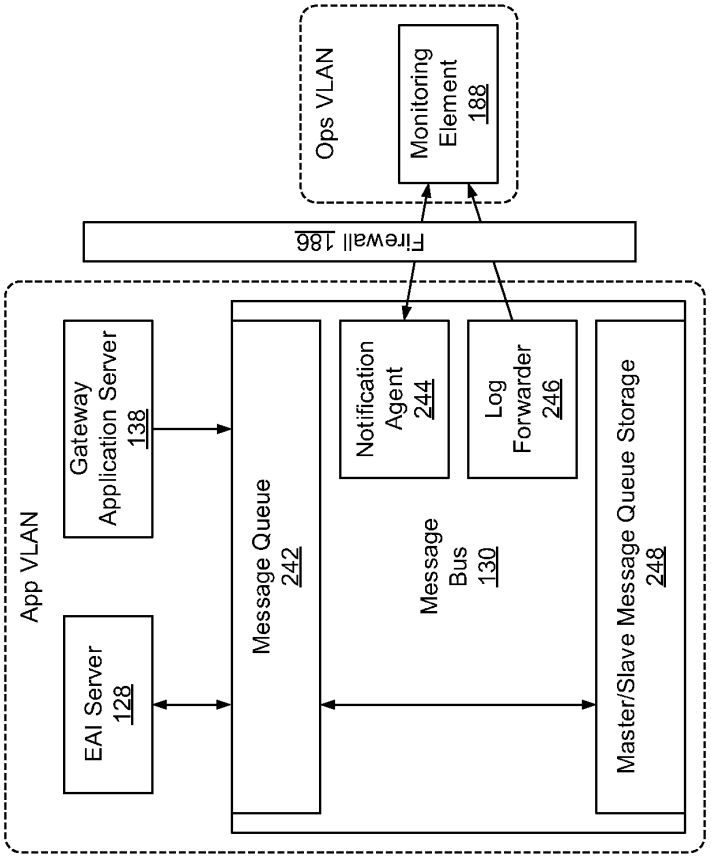

Ops VLAN
Monitoring Element 188
Firewall 186
App VLAN
Gateway Application Server 138
EAI Server 128
Message Queue 242
Notification Agent 244
Log Forwarder 246
Message Bus 130
Master/Slave Message Queue Storage 248

FIG. 19

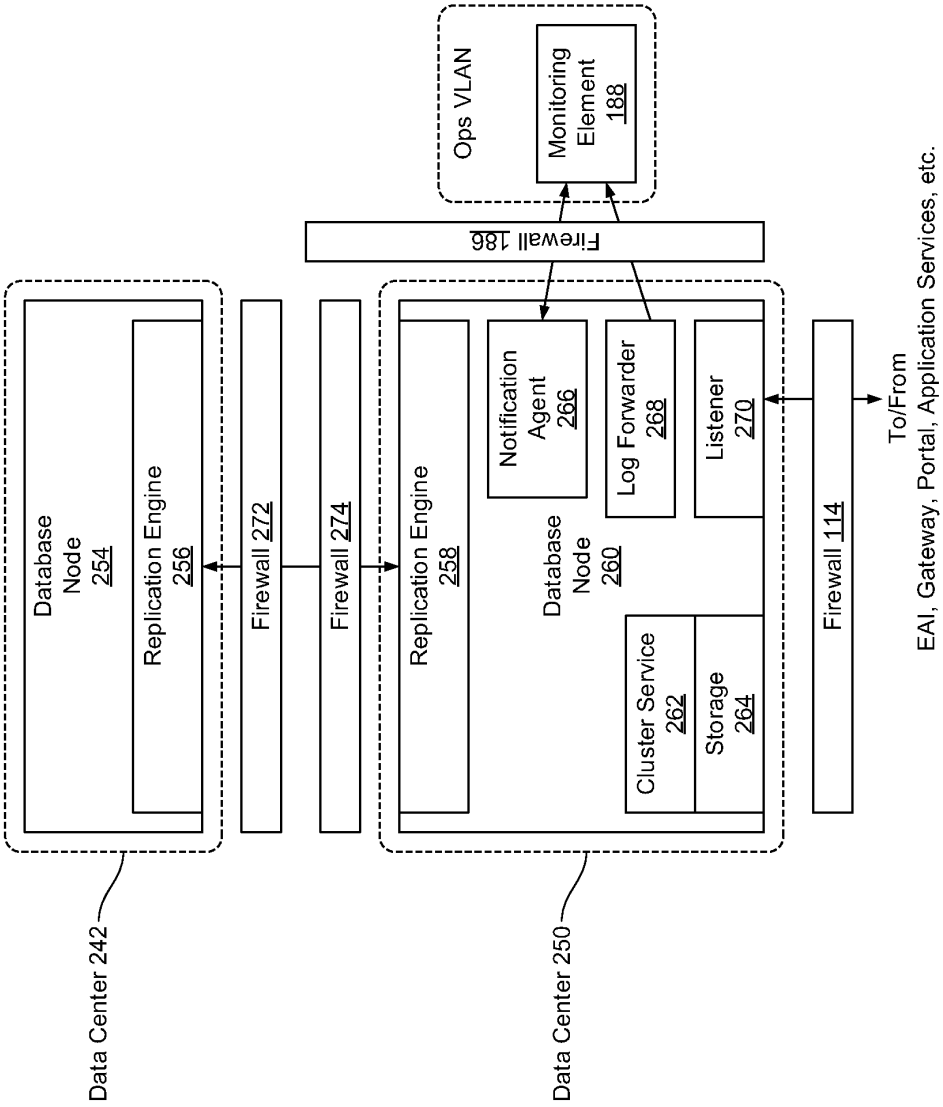

Ops VLAN
Monitoring Element 188
Firewall 186
Database Node 254
Replication Engine 256
Firewall 272
Firewall 274
Replication Engine 258
Notification Agent 266
Log Forwarder 268
Listener 270
Database Node 260
Cluster Service 262
Storage 264
Firewall 114
To/From
EAI, Gateway, Portal, Application Services, etc.
Data Center 242
Data Center 250

FIG. 20

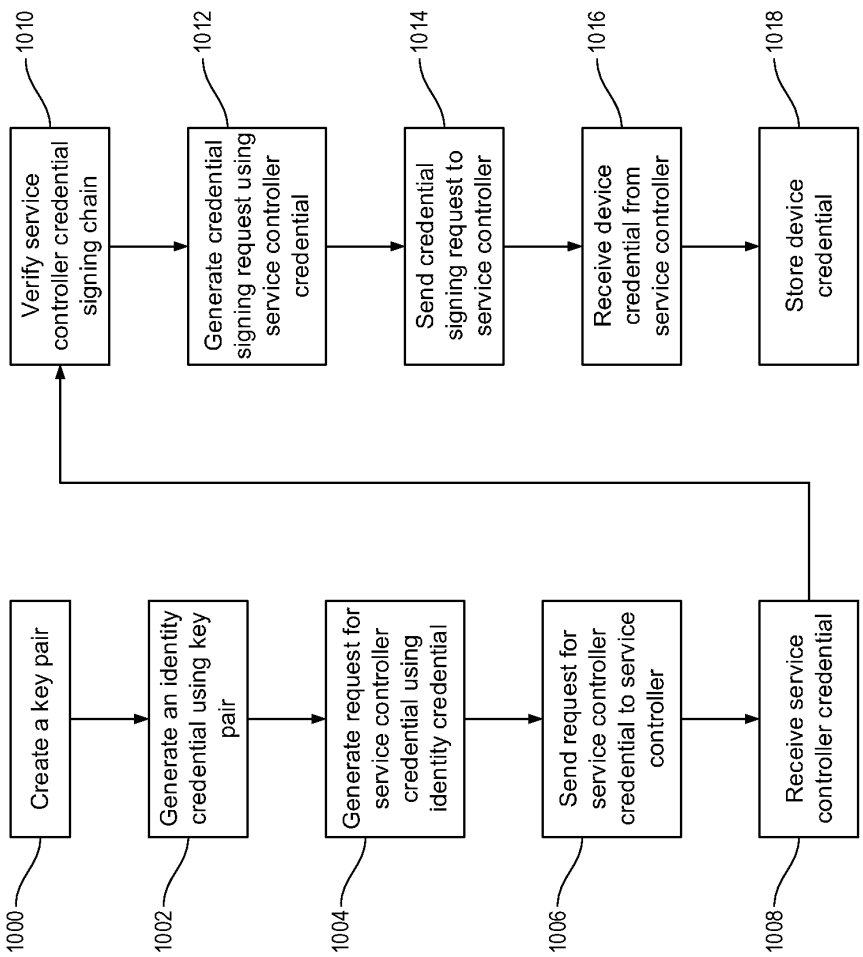

1000
Create a key pair
1002
Generate an identity credential using key pair
1004
Generate request for service controller credential using identity credential
1006
Send request for service controller credential to service controller
1008
Receive service controller credential
1010
Verify service controller credential signing chain
1012
Generate credential signing request using service controller credential
1014
Send credential signing request to service controller
1016
Receive device credential from service controller
1018
Store device credential

FIG. 21

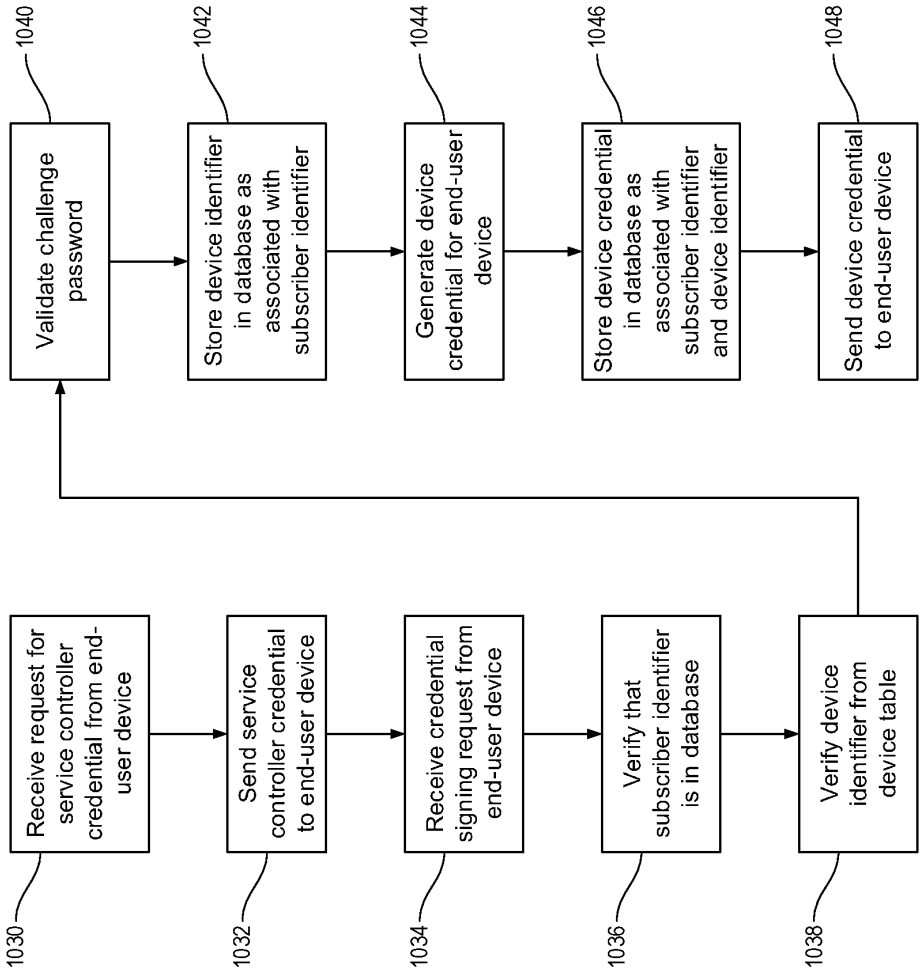

1030
Receive request for service controller credential from end-user device
1032
Send service controller credential to end-user device
1034
Receive credential signing request from end-user device
1036
Verify that subscriber identifier is in database
1038
Verify device identifier from device table
1040
Validate challenge password
1042
Store device identifier in database as associated with subscriber identifier
1044
Generate device credential for end-user device
1046
Store device credential in database as associated with subscriber identifier and device identifier
1048
Send device credential to end-user device

FIG. 22

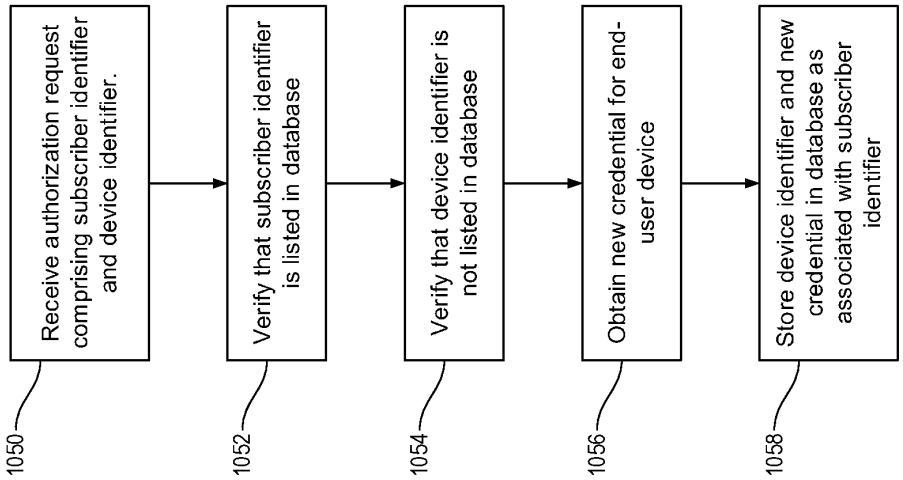

Receive authorization request comprising subscriber identifier and device identifier.
Verify that subscriber identifier is listed in database
Verify that device identifier is not listed in database
Obtain new credential for end-user device
Store device identifier and new credential in database as associated with subscriber identifier
1050
1052
1054
1056
1058

FIG. 23

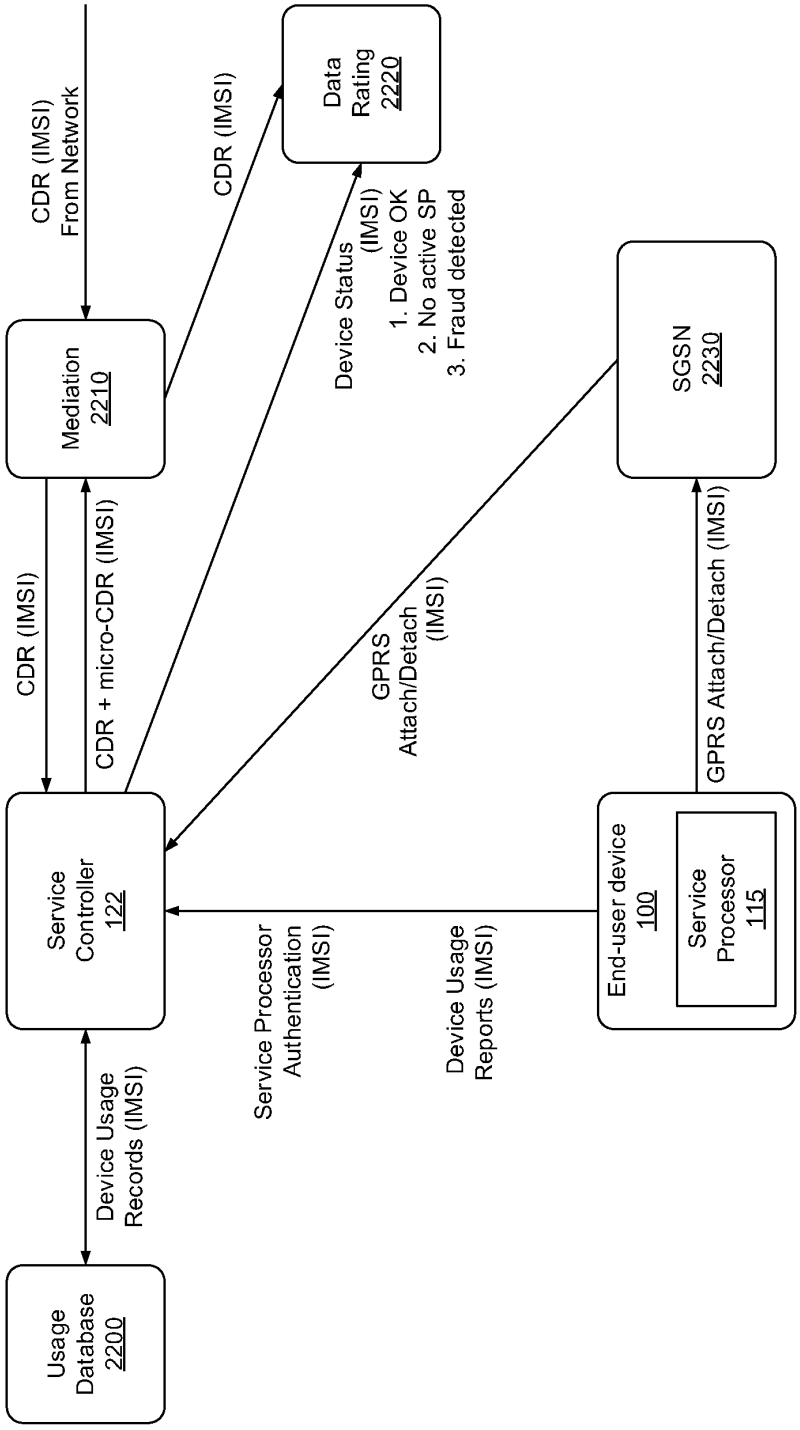

CDR (IMSI)
From Network
Mediation
2210
CDR (IMSI)
Data
Rating
2220
Device Status
(IMSI)
1. Device OK
2. No active SP
3. Fraud detected
CDR (IMSI)
CDR + micro-CDR (IMSI)
GPRS
Attach/Detach
(IMSI)
SGSN
2230
Service
Controller
122
GPRS Attach/Detach (IMSI)
End-user device
100
Service
Processor
115
Service Processor
Authentication
(IMSI)
Device Usage
Reports (IMSI)
Device Usage
Records (IMSI)
Usage
Database
2200

FIG. 24

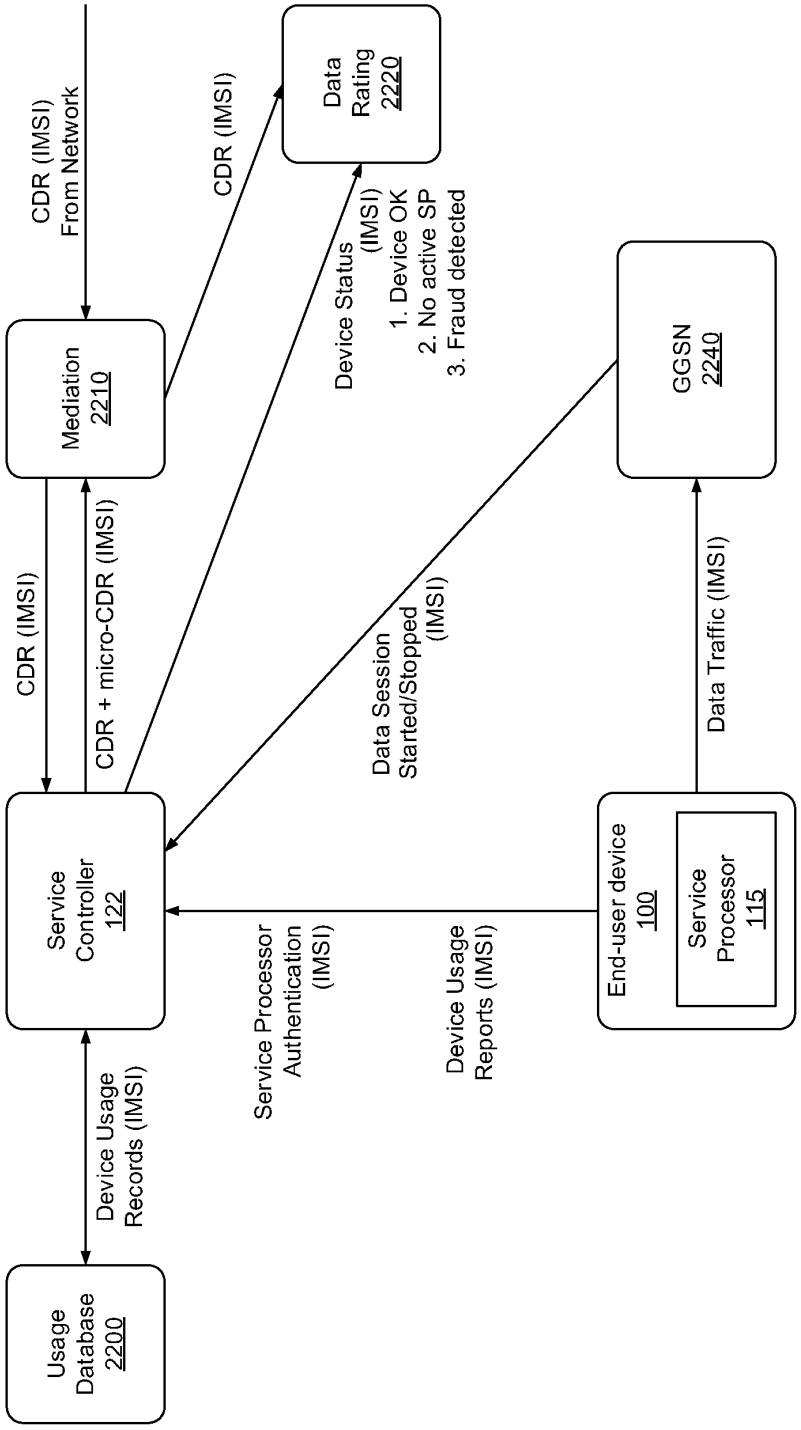

CDR (IMSI)
From Network
Mediation
2210
CDR (IMSI)
Data
Rating
2220
Device Status
(IMSI)
1. Device OK
2. No active SP
3. Fraud detected
CDR (IMSI)
CDR + micro-CDR (IMSI)
Service
Controller
122
Data Session
Started/Stopped
(IMSI)
GGSN
2240
Data Traffic (IMSI)
Service Processor
Authentication
(IMSI)
Device Usage
Reports (IMSI)
End-user device
100
Service
Processor
115
Device Usage
Records (IMSI)
Usage
Database
2200

FIG. 25

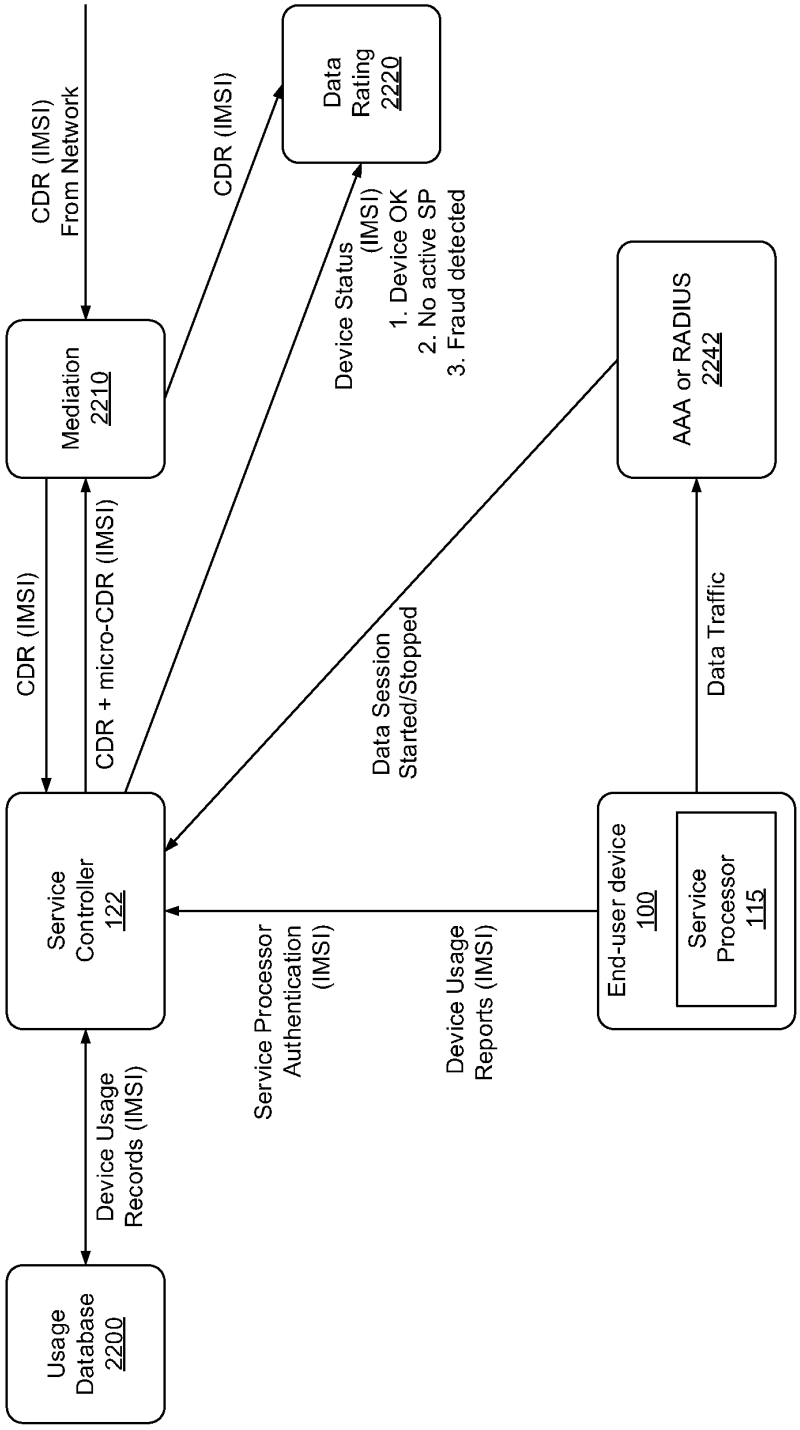

CDR (IMSI)
From Network
Mediation
2210
CDR (IMSI)
Data
Rating
2220
Device Status
(IMSI)
1. Device OK
2. No active SP
3. Fraud detected
CDR (IMSI)
CDR + micro-CDR (IMSI)
Service
Controller
122
Data Session
Started/Stopped
AAA or RADIUS
2242
Data Traffic
Service Processor
Authentication
(IMSI)
Device Usage
Reports (IMSI)
End-user device
100
Service
Processor
115
Device Usage
Records (IMSI)
Usage
Database
2200

FIG. 26

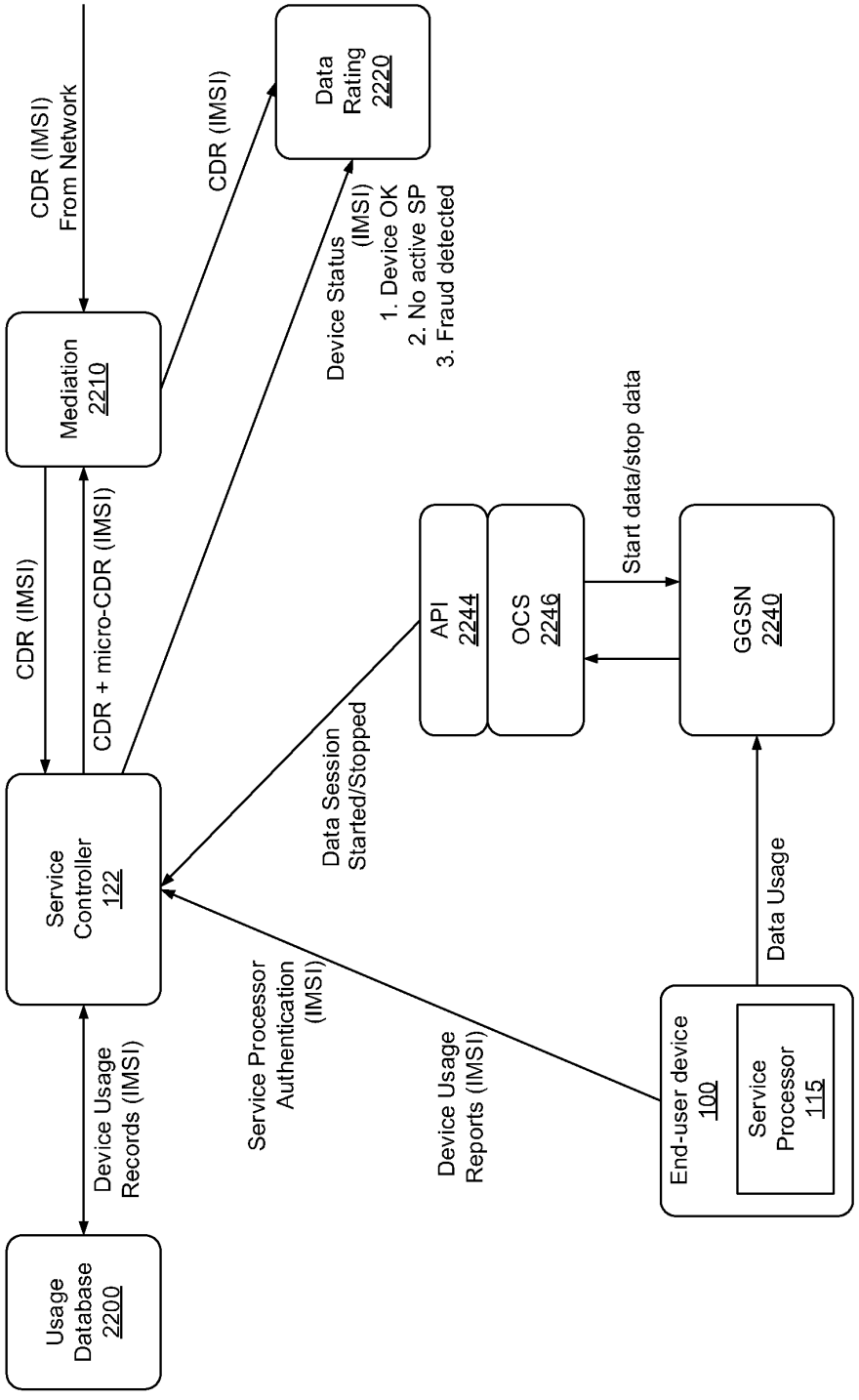

CDR (IMSI)
From Network
Mediation
2210
CDR (IMSI)
Data
Rating
2220
Device Status
(IMSI)
1. Device OK
2. No active SP
3. Fraud detected
CDR (IMSI)
CDR + micro-CDR (IMSI)
API
2244
OCS
2246
Start data/stop data
GGSN
2240
Service
Controller
122
Data Session
Started/Stopped
Service Processor
Authentication
(IMSI)
Device Usage
Reports (IMSI)
Data Usage
Device Usage
Records (IMSI)
End-user device
100
Service
Processor
115
Usage
Database
2200

FIG. 27

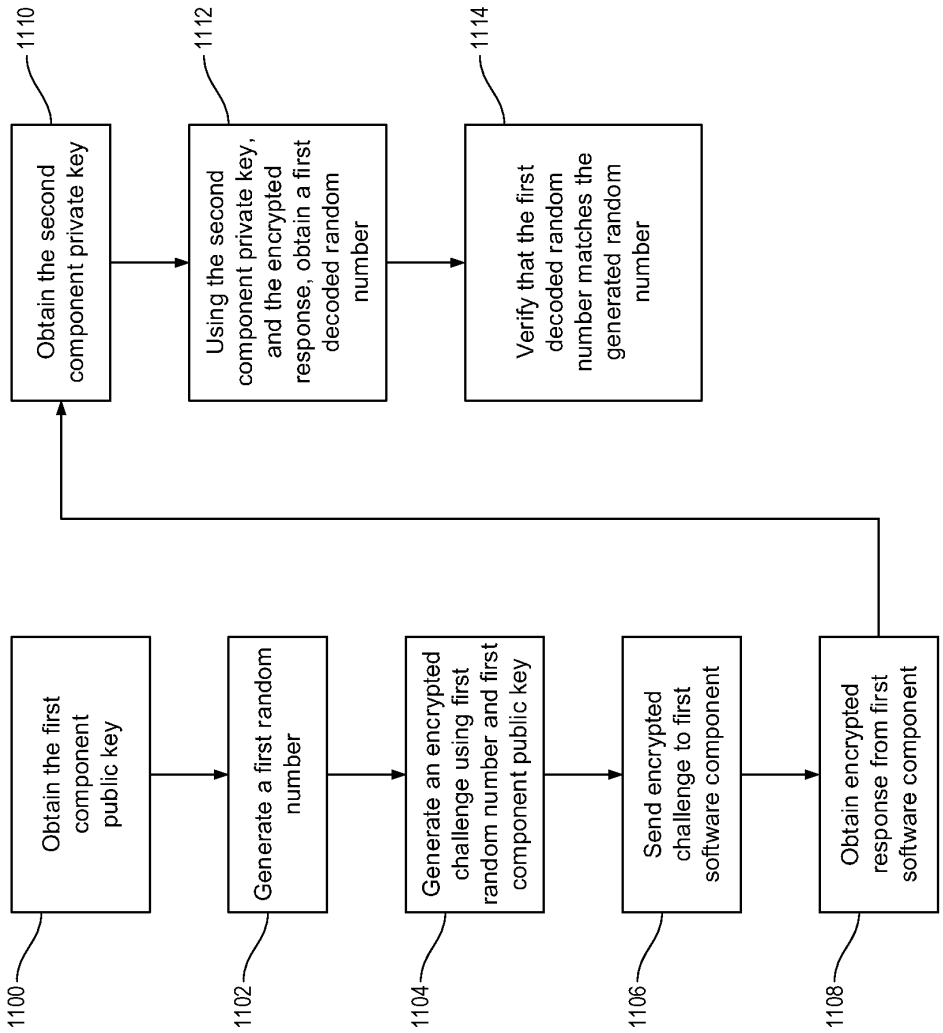

Obtain the first component public key
Generate a first random number
Generate an encrypted challenge using first random number and first component public key
Send encrypted challenge to first software component
Obtain encrypted response from first software component
Obtain the second component private key
Using the second component private key, and the encrypted response, obtain a first decoded random number
Verify that the first decoded random number matches the generated random number
1100
1102
1104
1106
1108
1110
1112
1114

FIG. 28

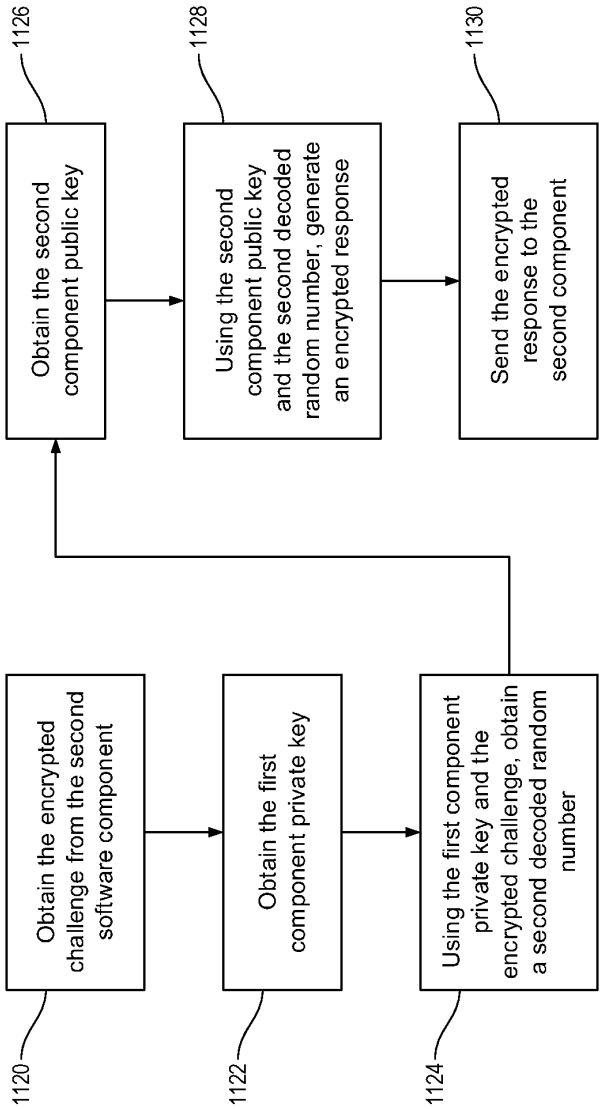

1126
1128
1130
Obtain the second component public key
Using the second component public key and the second decoded random number, generate an encrypted response
Send the encrypted response to the second component
Obtain the encrypted challenge from the second software component
Obtain the first component private key
Using the first component private key and the encrypted challenge, obtain a second decoded random number
1120
1122
1124

FIG. 29

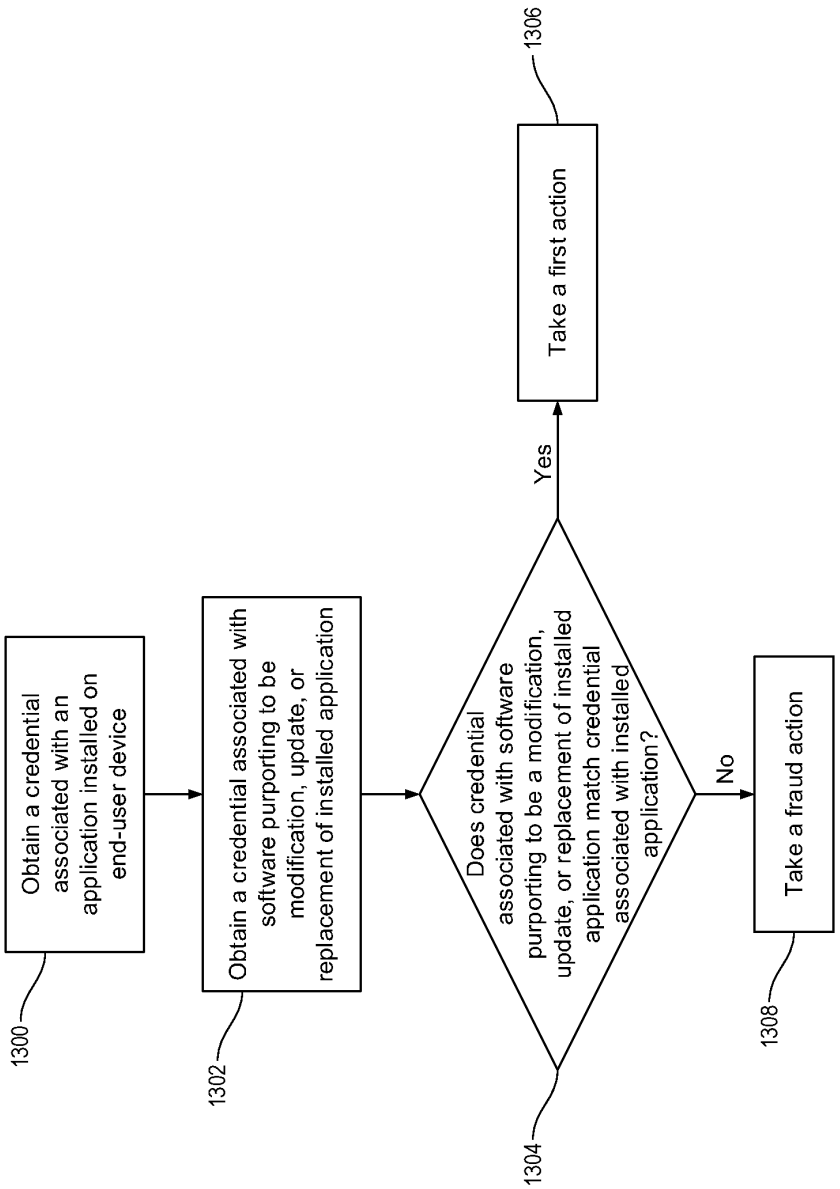

Obtain a credential associated with an application installed on end-user device
1300
Obtain a credential associated with software purporting to be modification, update, or replacement of installed application
1302
Does credential associated with software purporting to be a modification, update, or replacement of installed application match credential associated with installed application?
1304
Yes
Take a first action
1306
No
Take a fraud action
1308

FIG. 30

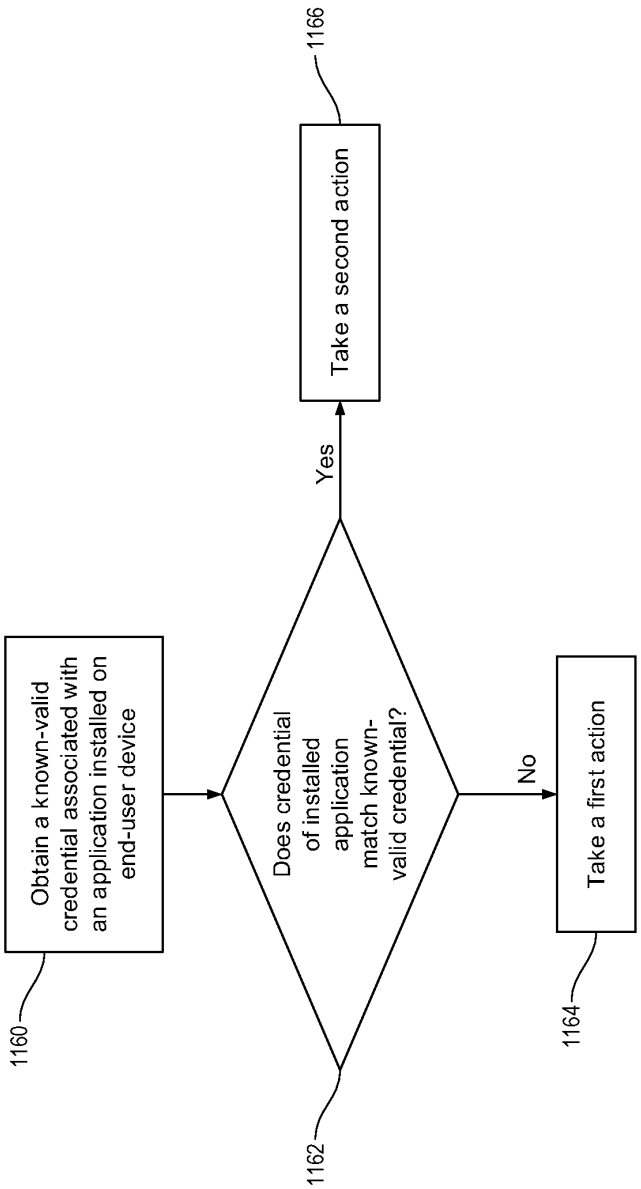

Obtain a known-valid credential associated with an application installed on end-user device
1160
Does credential of installed application match known-valid credential?
1162
Yes
Take a second action
1166
No
Take a first action
1164

FIG. 31

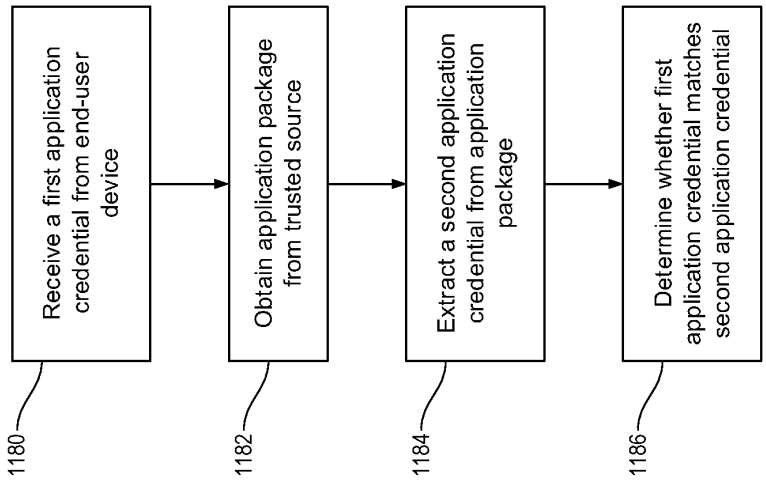

Receive a first application credential from end-user device
Obtain application package from trusted source
Extract a second application credential from application package
Determine whether first application credential matches second application credential
1180
1182
1184
1186

FIG. 33

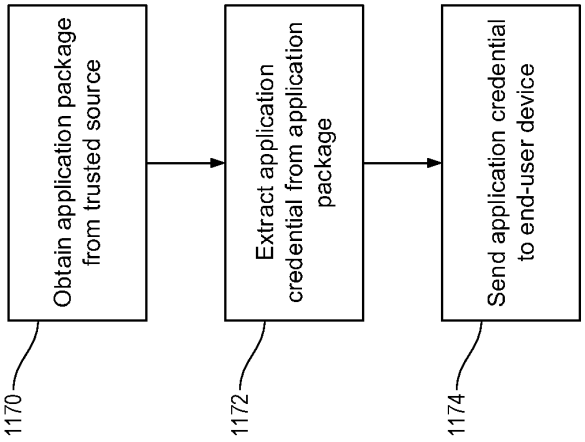

Obtain application package from trusted source
Extract application credential from application package
Send application credential to end-user device
1170
1172
1174

FIG. 32

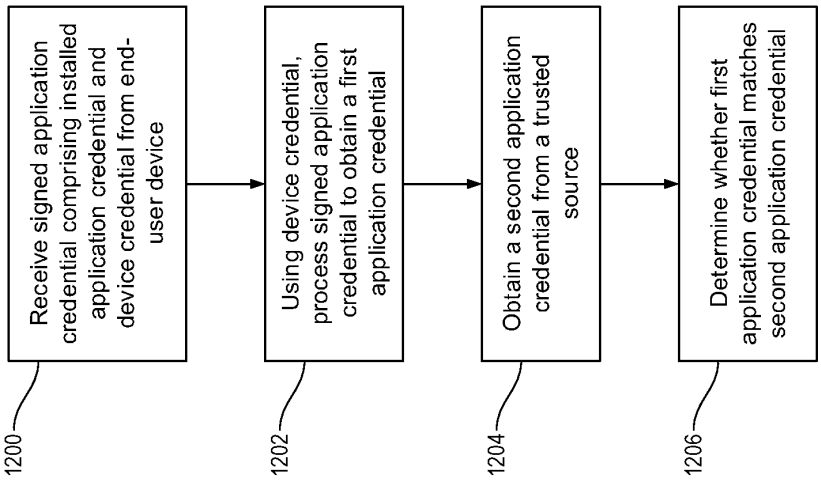

Receive signed application credential comprising installed application credential and device credential from end-user device
Using device credential, process signed application credential to obtain a first application credential
Obtain a second application credential from a trusted source
Determine whether first application credential matches second application credential
1200
1202
1204
1206

FIG. 35

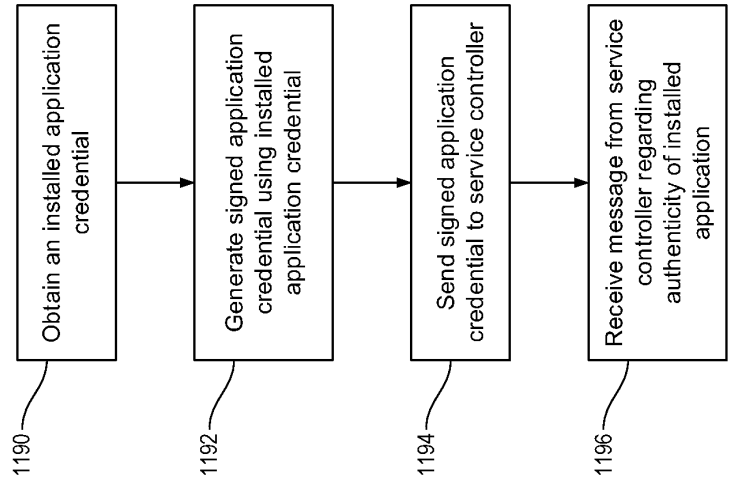

Obtain an installed application credential
Generate signed application credential using installed application credential
Send signed application credential to service controller
Receive message from service controller regarding authenticity of installed application
1190
1192
1194
1196

FIG. 34

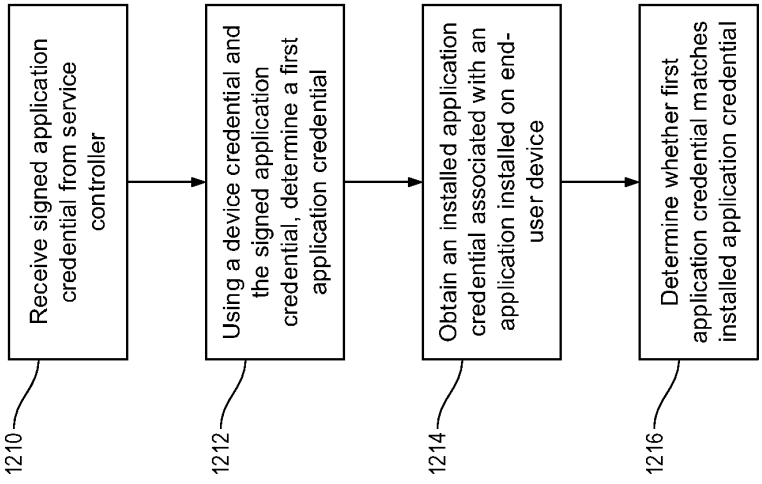

Receive signed application credential from service controller
Using a device credential and the signed application credential, determine a first application credential
Obtain an installed application credential associated with an application installed on end-user device
Determine whether first application credential matches installed application credential
1210
1212
1214
1216

FIG. 36

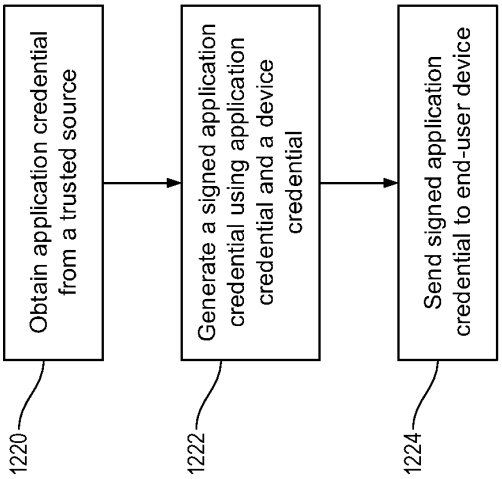

Obtain application credential from a trusted source
Generate a signed application credential using application credential and a device credential
Send signed application credential to end-user device
1220
1222
1224

FIG. 37

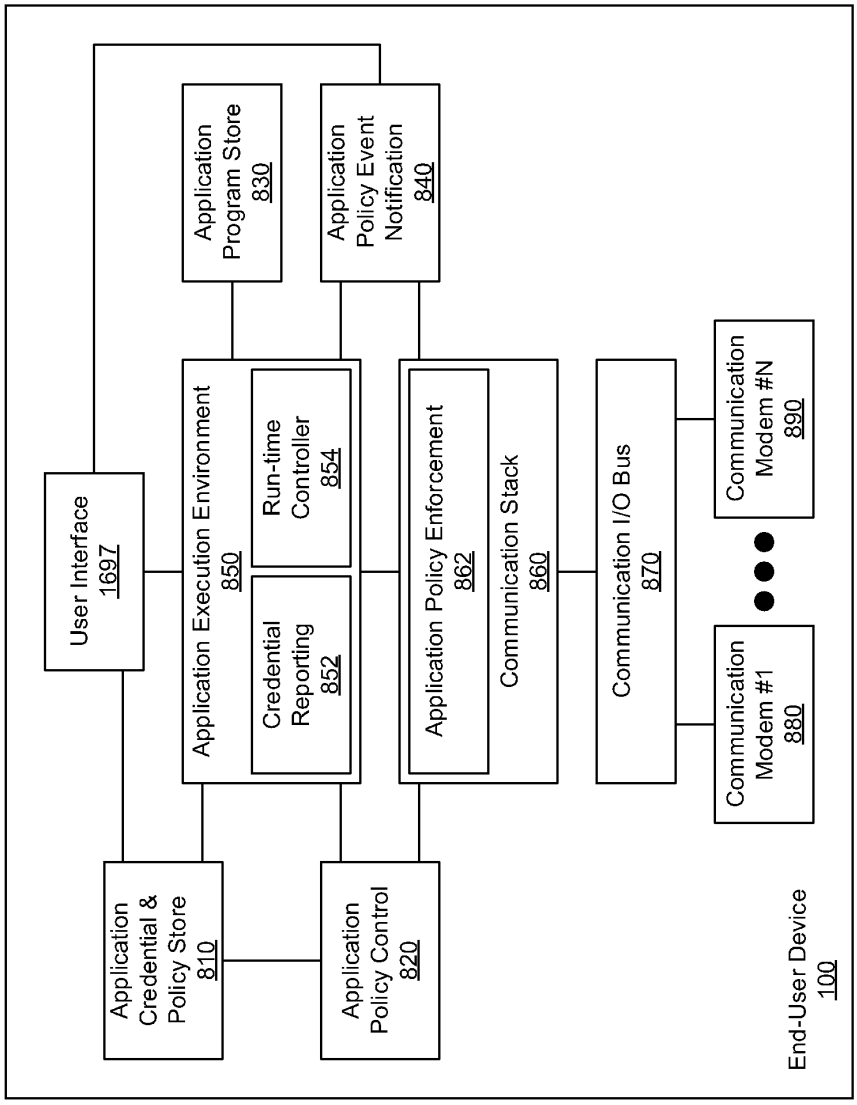

End-User Device
100
User Interface
1697
Application
Credential &
Policy Store
810
Application
Policy Control
820
Application Execution Environment
850
Credential
Reporting
852
Run-time
Controller
854
Application
Program Store
830
Application
Policy Event
Notification
840
Application Policy Enforcement
862
Communication Stack
860
Communication I/O Bus
870
Communication
Modem #1
880
Communication
Modem #N
890

FIG. 38

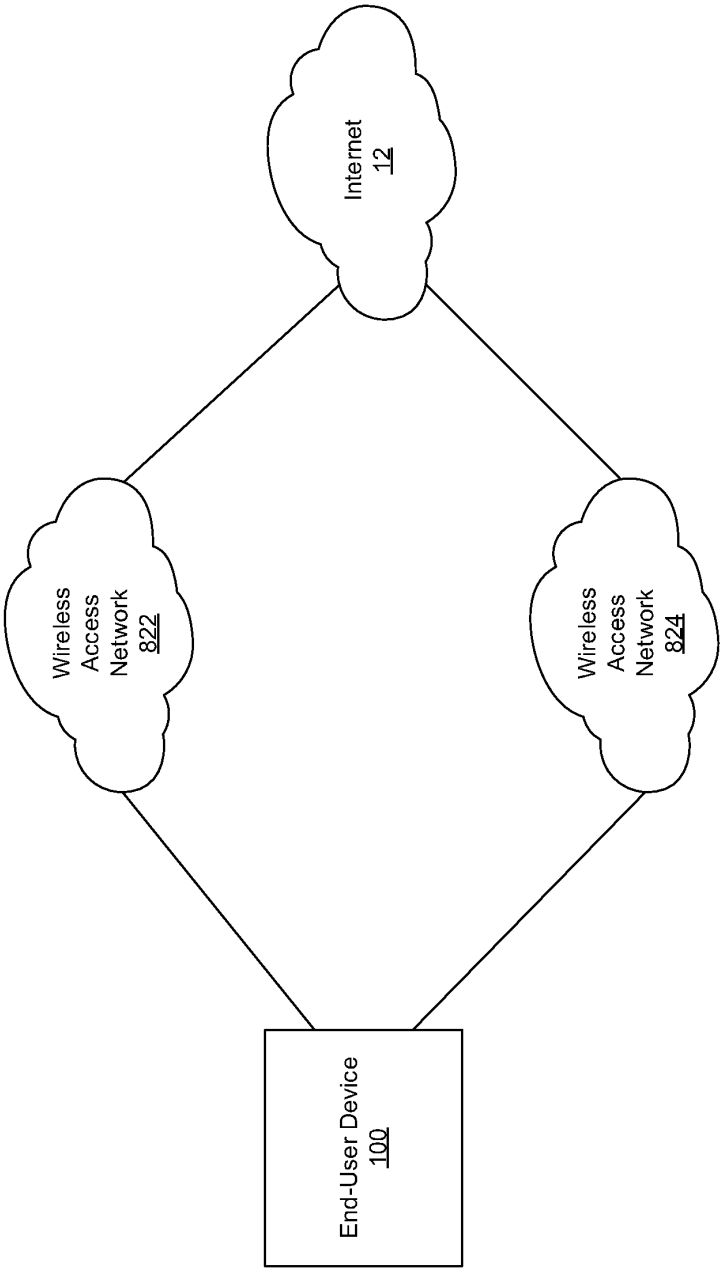

Internet
12
Wireless
Access
Network
822
Wireless
Access
Network
824
End-User Device
100

FIG. 39

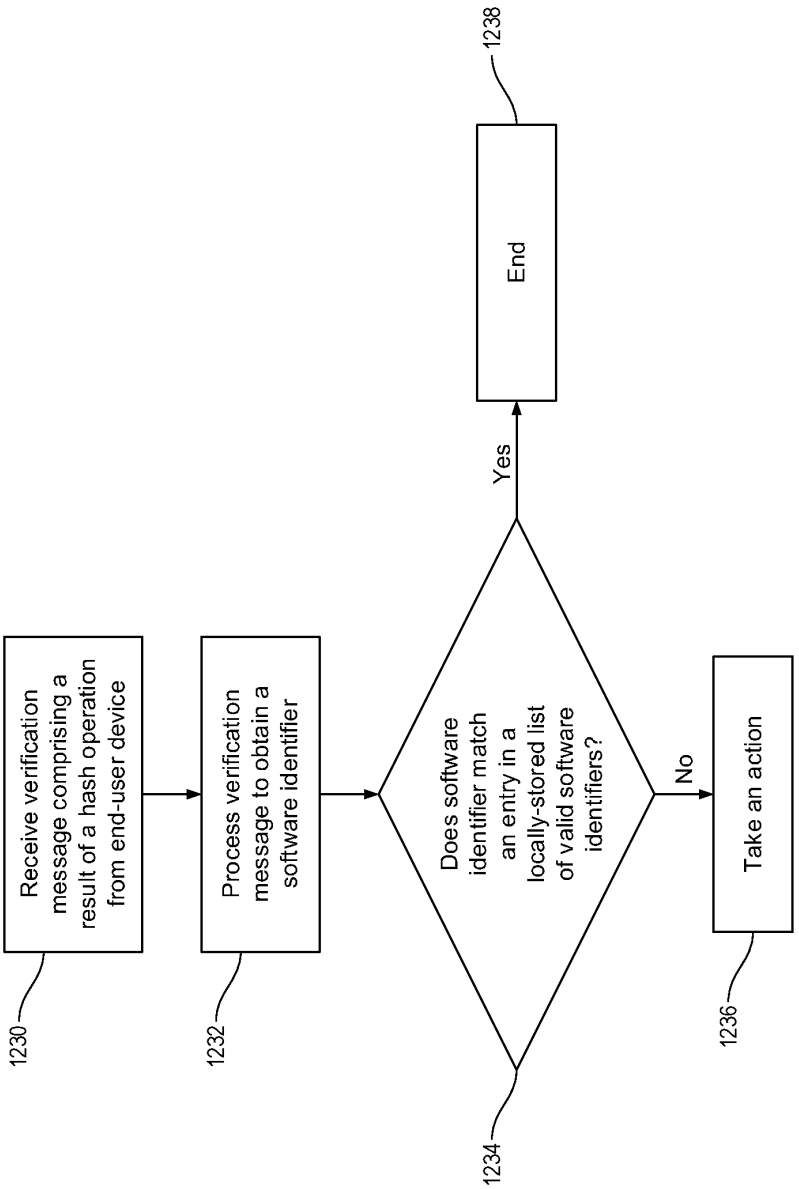

Receive verification message comprising a result of a hash operation from end-user device
1230
Process verification message to obtain a software identifier
1232
Does software identifier match an entry in a locally-stored list of valid software identifiers?
1234
Yes
End
1238
No
Take an action
1236

FIG. 40

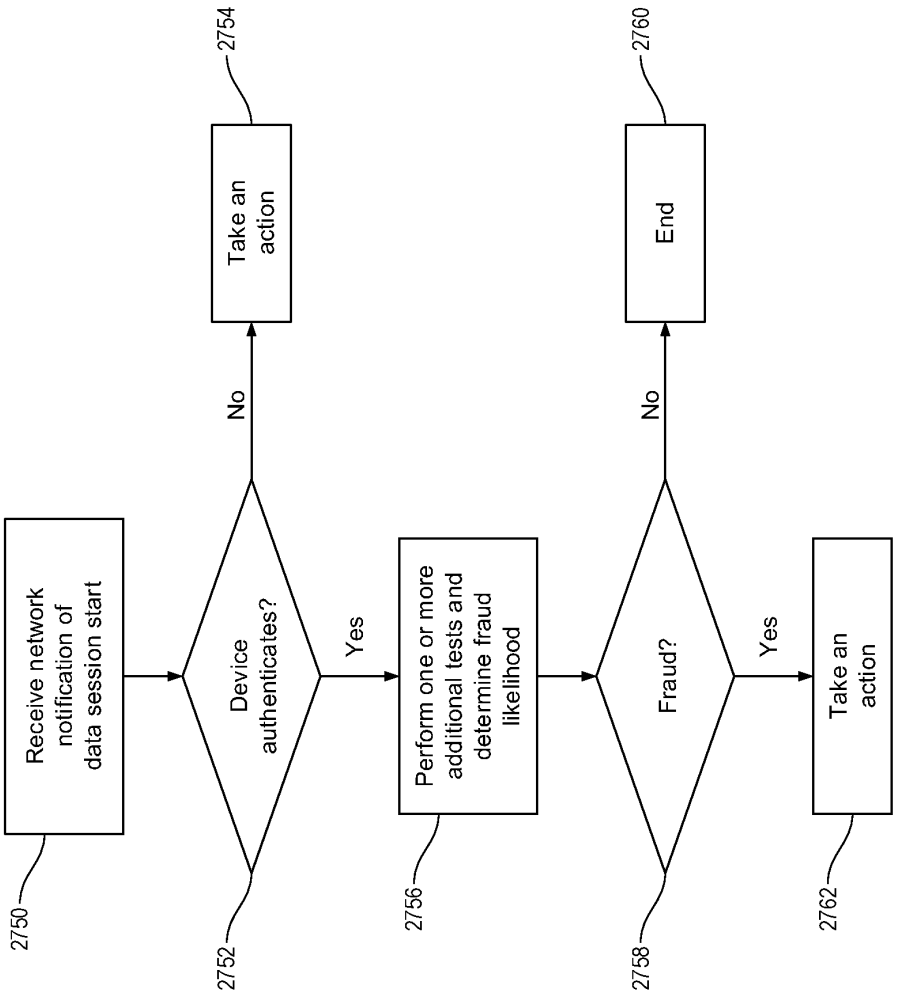

Receive network notification of data session start
2750
Device authenticates?
2752
No
Take an action
2754
Yes
Perform one or more additional tests and determine fraud likelihood
2756
Fraud?
2758
No
End
2760
Yes
Take an action
2762

FIG. 41

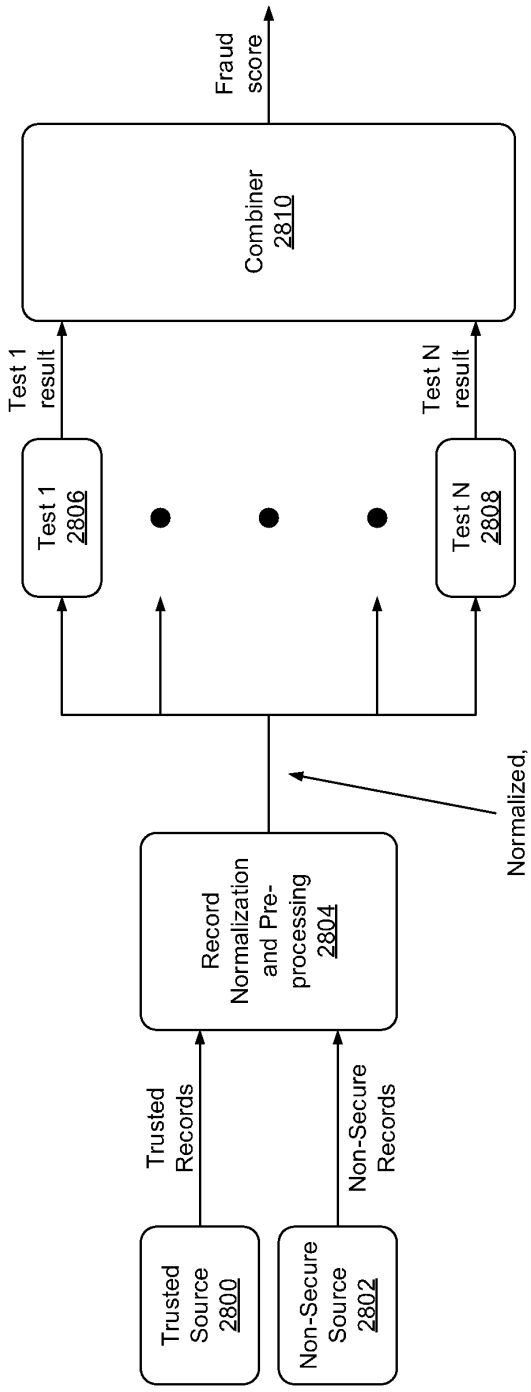

Trusted Source 2800
Non-Secure Source 2802
Trusted Records
Non-Secure Records
Record Normalization and Pre-processing 2804
Normalized, pre-processed trusted records and non-secure records
Test 1 2806
Test N 2808
Test 1 result
Test N result
Combiner 2810
Fraud score

FIG. 42

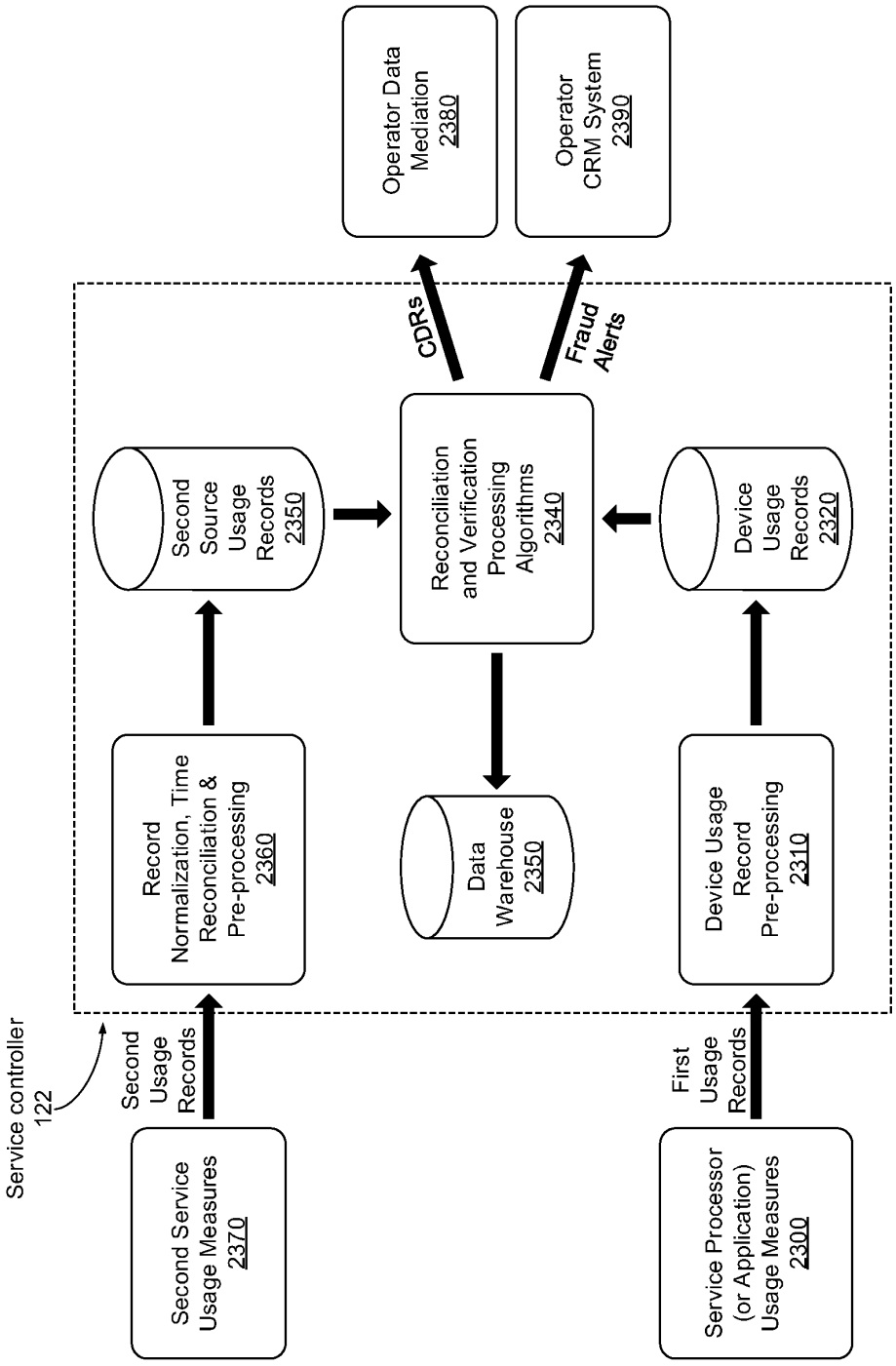

Service controller 122
Second Usage Records
First Usage Records
Second Service Usage Measures 2370
Service Processor (or Application) Usage Measures 2300
Record Normalization, Time Reconciliation & Pre-processing 2360
Device Usage Record Pre-processing 2310
Second Source Usage Records 2350
Data Warehouse 2350
Device Usage Records 2320
Reconciliation and Verification Processing Algorithms 2340
CDRs
Fraud Alerts
Operator Data Mediation 2380
Operator CRM System 2390

FIG. 43

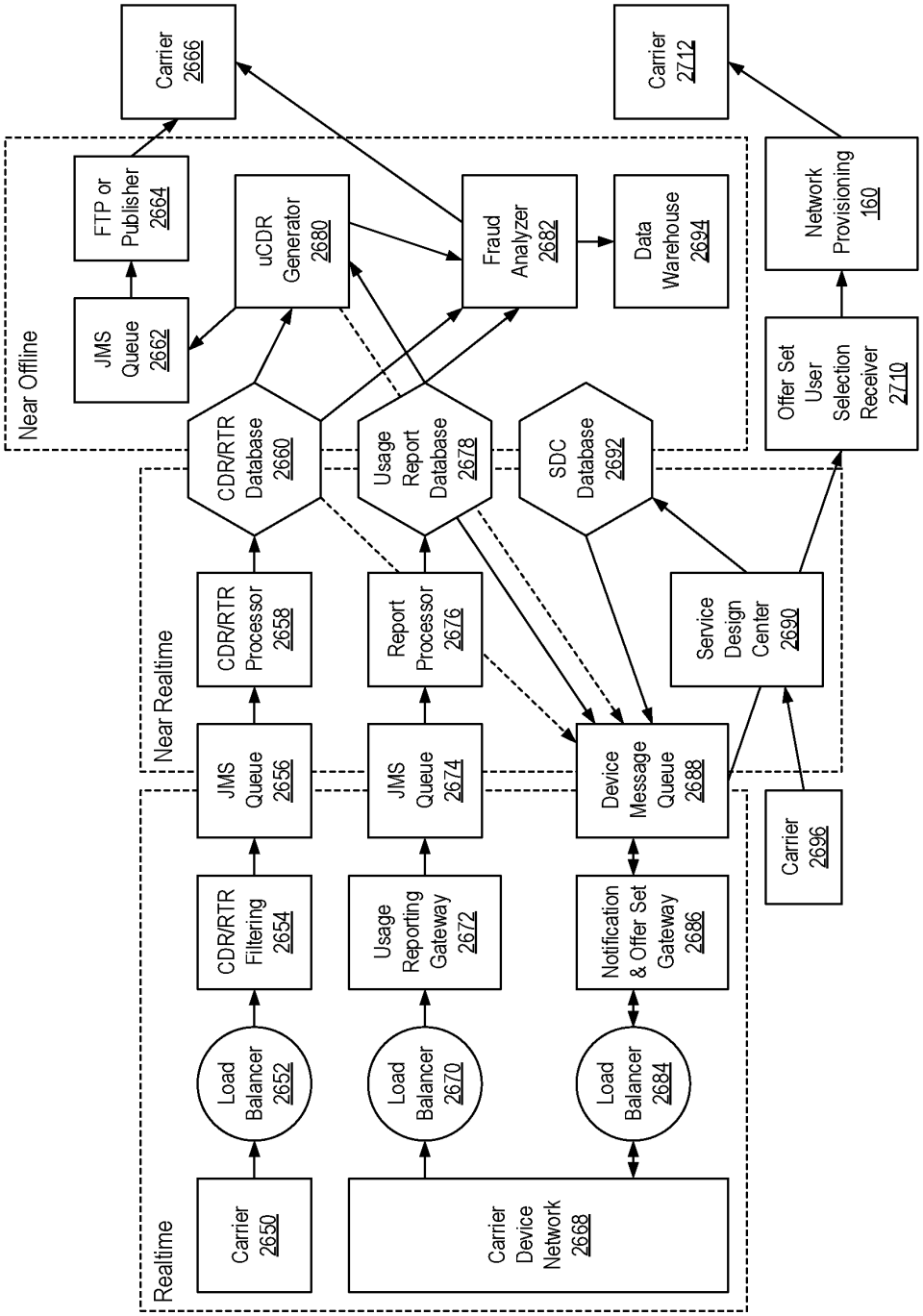

Carrier 2666
Carrier 2712
FTP or Publisher 2664
uCDR Generator 2680
Fraud Analyzer 2682
Data Warehouse 2694
Network Provisioning 160
Near Offline
JMS Queue 2662
Offer Set User Selection Receiver 2710
CDR/RTR Database 2660
Usage Report Database 2678
SDC Database 2692
Near Realtime
CDR/RTR Processor 2658
Report Processor 2676
Service Design Center 2690
JMS Queue 2656
JMS Queue 2674
Device Message Queue 2688
Carrier 2696
CDR/RTR Filtering 2654
Usage Reporting Gateway 2672
Notification & Offer Set Gateway 2686
Load Balancer 2652
Load Balancer 2670
Load Balancer 2684
Realtime
Carrier 2650
Carrier Device Network 2668

FIG. 44

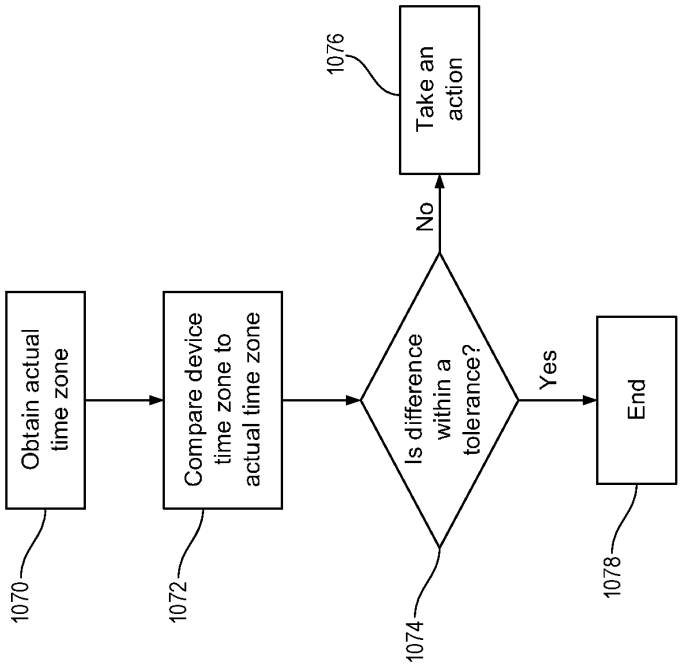

Obtain actual time zone
Compare device time zone to actual time zone
Is difference within a tolerance?
No
Take an action
Yes
End
1070
1072
1074
1076
1078

FIG. 46

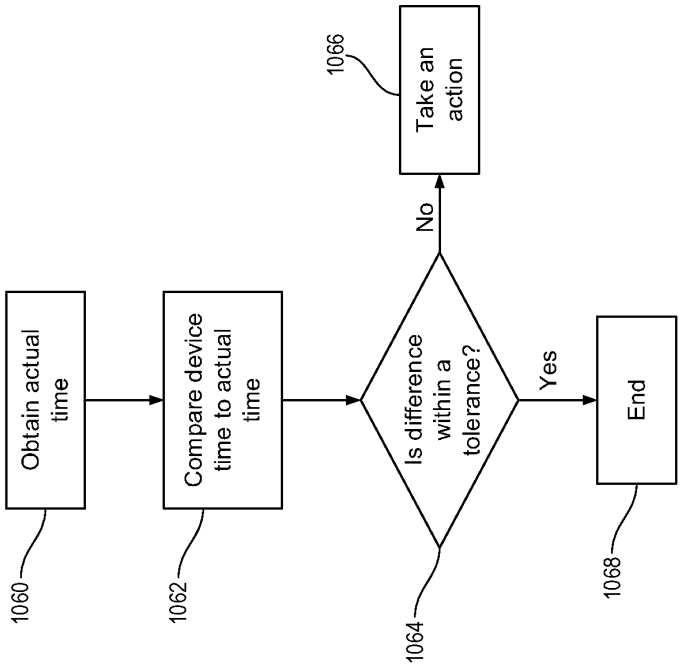

Obtain actual time
Compare device time to actual time
Is difference within a tolerance?
No
Take an action
Yes
End
1060
1062
1064
1066
1068

FIG. 45

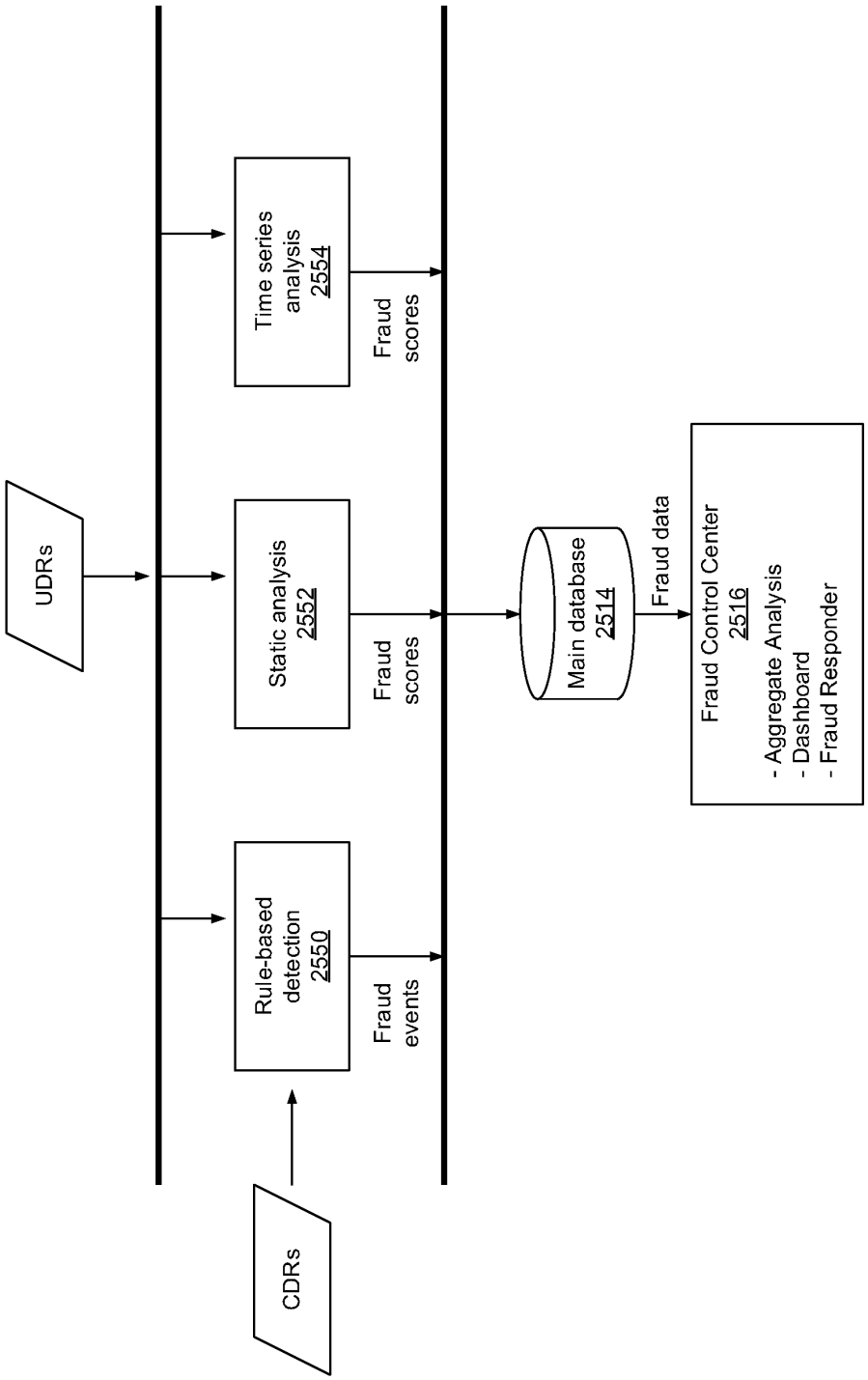

CDRs
UDRs
Rule-based detection 2550
Static analysis 2552
Time series analysis 2554
Fraud events
Fraud scores
Fraud scores
Fraud scores
Main database 2514
Fraud data
Fraud Control Center 2516
- Aggregate Analysis
- Dashboard
- Fraud Responder

FIG. 47

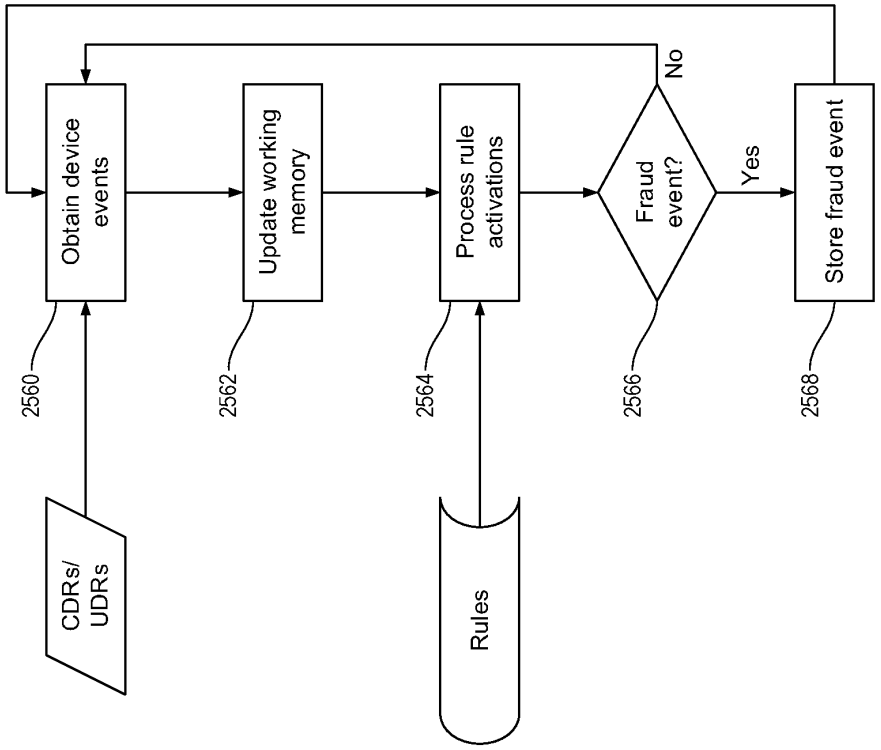

Obtain device events
Update working memory
Process rule activations
Fraud event?
No
Yes
Store fraud event
CDRs/ UDRs
Rules
2560
2562
2564
2566
2568

FIG. 48

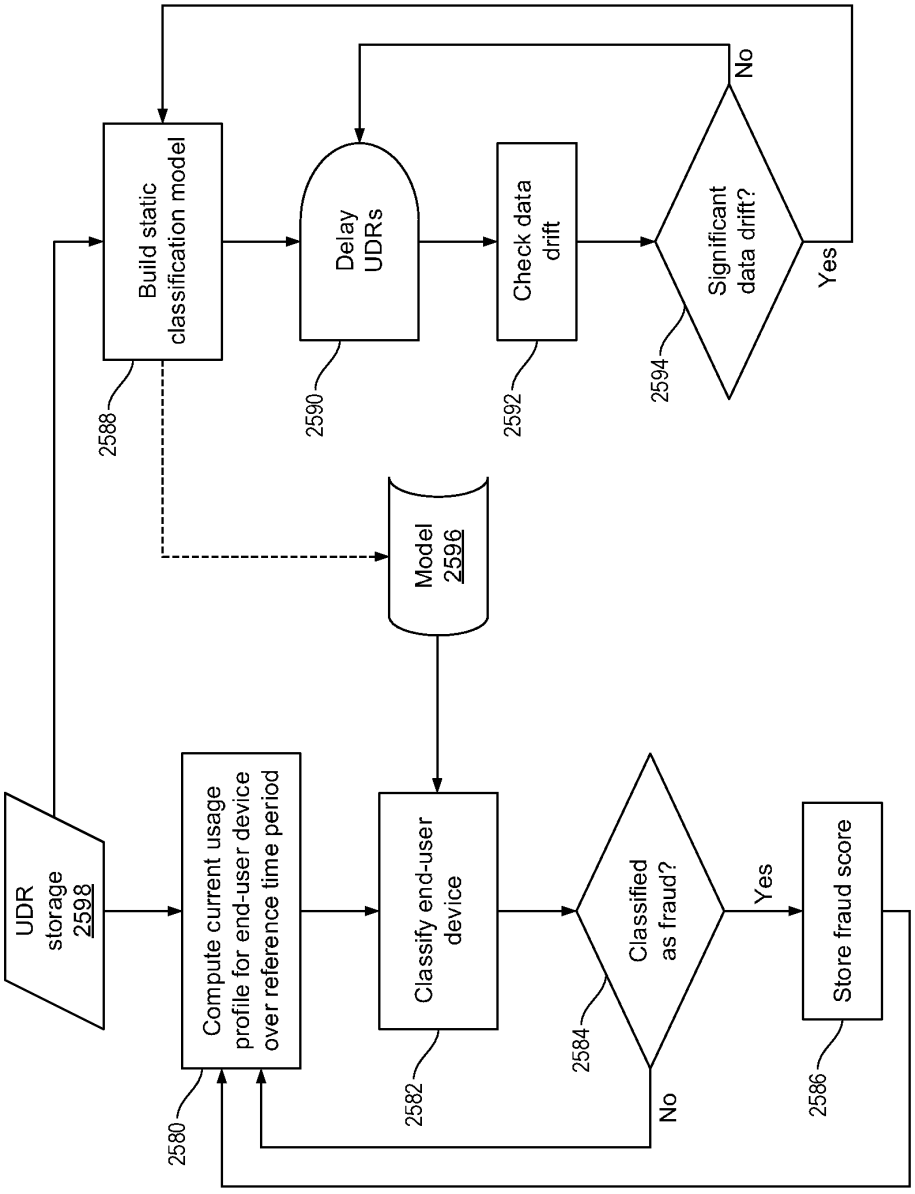

UDR storage 2598
Compute current usage profile for end-user device over reference time period
2580
Classify end-user device
2582
Classified as fraud?
2584
Yes
No
Store fraud score
2586
Model 2596
Build static classification model
2588
Delay UDRs
2590
Check data drift
2592
Significant data drift?
2594
Yes
No

FIG. 49

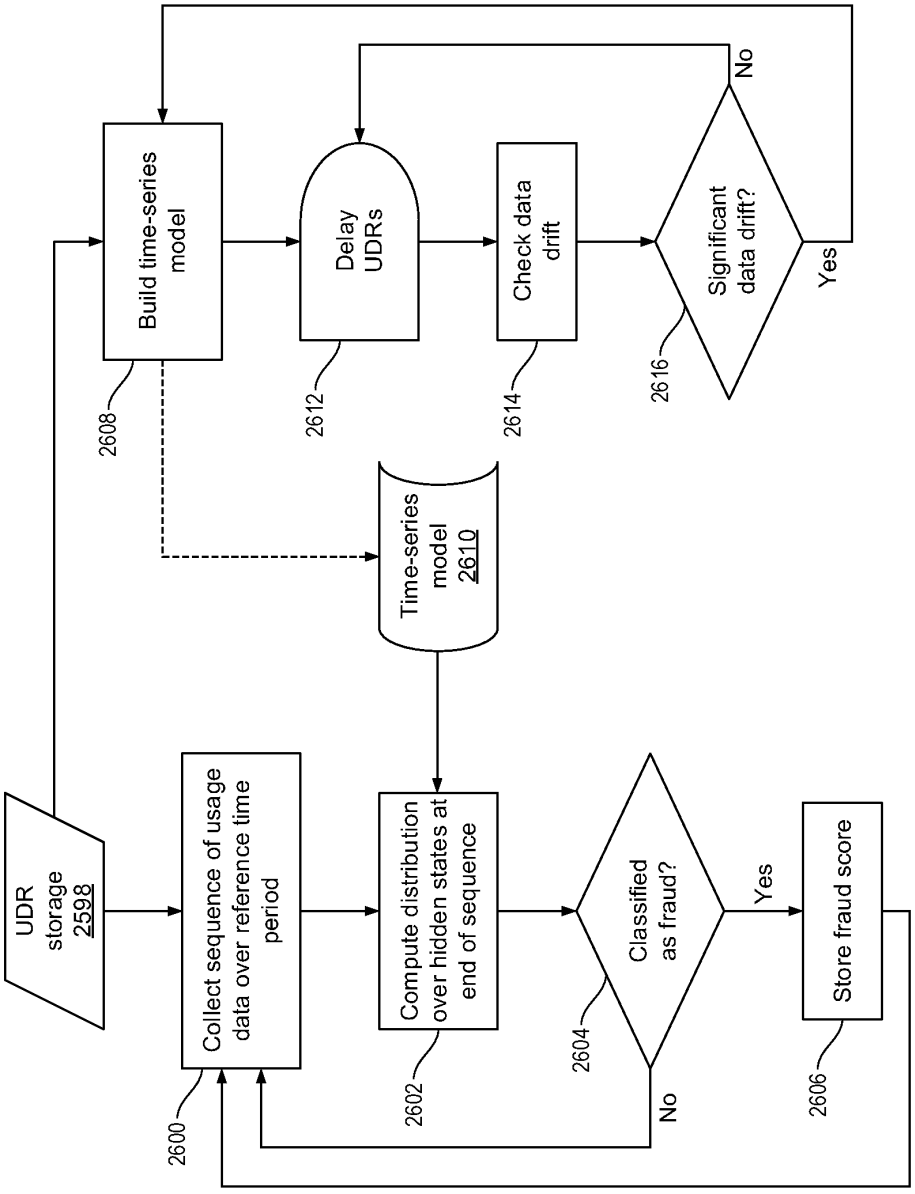

UDR storage 2598
Collect sequence of usage data over reference time period
2600
Compute distribution over hidden states at end of sequence
2602
Classified as fraud?
2604
Yes
No
Store fraud score
2606
Time-series model 2610
Build time-series model
2608
Delay UDRs
2612
Check data drift
2614
Significant data drift?
2616
Yes
No

FIG. 50

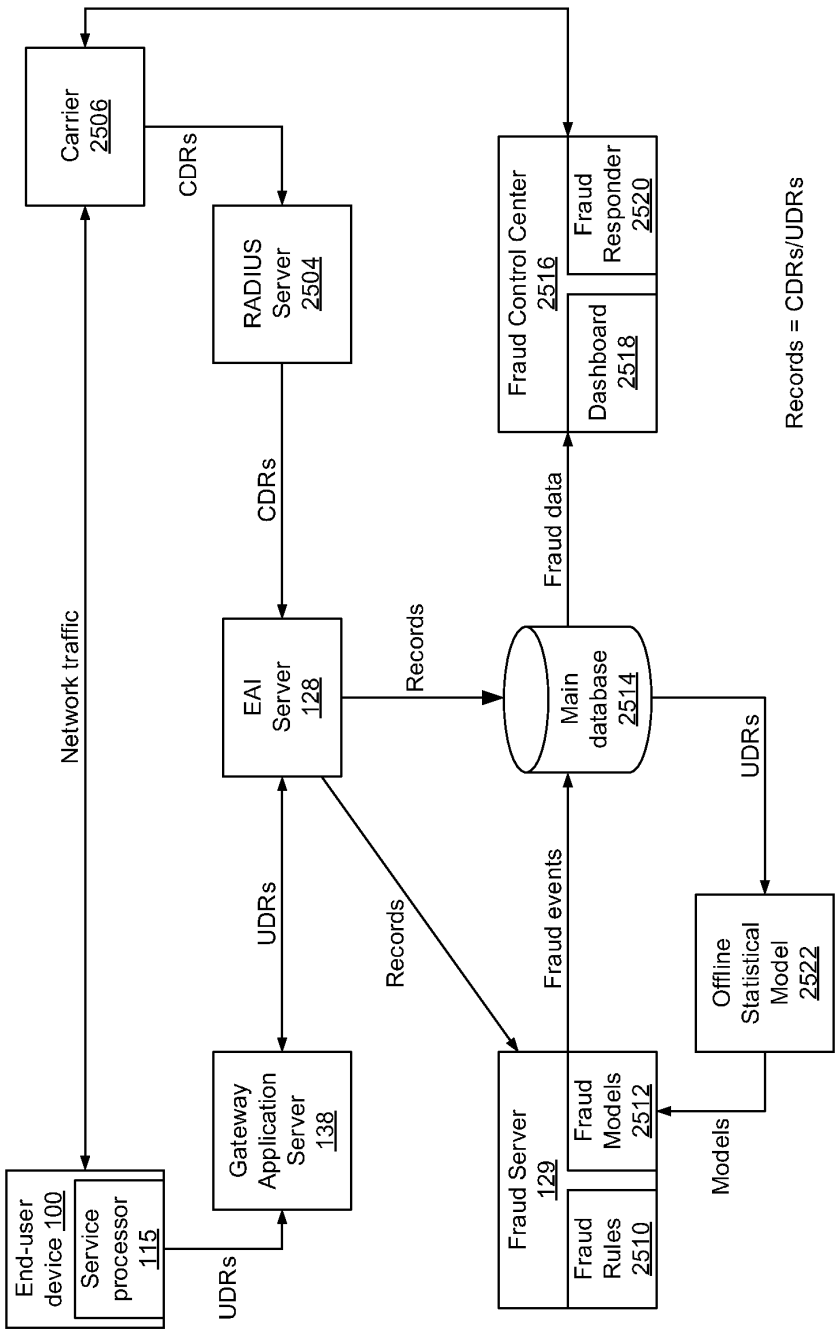

Carrier 2506
CDRs
RADIUS Server 2504
CDRs
EAI Server 128
Records
Main database 2514
Fraud data
Fraud Control Center 2516
Fraud Responder 2520
Dashboard 2518
Records = CDRs/UDRs
Network traffic
UDRs
Records
Fraud events
UDRs
Offline Statistical Model 2522
Gateway Application Server 138
Fraud Server 129
Fraud Models 2512
Fraud Rules 2510
Models
End-user device 100
Service processor 115
UDRs

FIG. 51

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

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.

WARNING:

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.

LEGAL NAME OF INVENTOR

Inventor: James Lavine Date (Optional): 6/17/14

Signature: _____

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.

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.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

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.

WARNING:

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.

LEGAL NAME OF INVENTOR

Inventor: Gregory G. Raleigh Date (Optional): _____

Signature: _____

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.

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.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

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.

WARNING:

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.

LEGAL NAME OF INVENTOR

Inventor: Jeffrey Green Date (Optional) : _____

Signature: _____

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.

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:	27148024
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	06-OCT-2016
Filing Date:	
Time Stamp:	19:13:49
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	Application Data Sheet	P041D1C1_ADS.pdf	1824865 ee1d7a48acf279b38e09600a56daeb452015e3b9	no	14
Warnings:					

Information:					
2		P041D1C1_App.pdf	677244 31c58aeff051efef86372baaa1936db9e3acc865	yes	157
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Specification		1	155	
	Claims		156	156	
	Abstract		157	157	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	P041D1C1_Drawings.pdf	1247989 361878f68d9661457e76c2bb5b53e80de33c6637	no	47
Warnings:					
Information:					
4	Oath or Declaration filed	P041D1C1_LavineDecl.pdf	642774 f0842df041edde36e2e6ccf62ad678fa9bf9dc97	no	1
Warnings:					
Information:					
5	Oath or Declaration filed	P041D1C1_RaleighDecl.pdf	637111 930a460d52e0fbd99c944345c22eb017e74cd957	no	1
Warnings:					
Information:					
6	Oath or Declaration filed	P041D1C1_GreenDecl.pdf	647170 6ec5647dcc21e412ec906d88481620ab9031dd61	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	5677153		

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1

CONFIRMATION NO. 4727

106963
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

FORMALITIES LETTER

OC000000086616892

Date Mailed: 10/21/2016

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.)

- $ **70** basic filing fee.
- $ **400** for **51** electronically equivalent pages in excess of **100** application size fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **1200** TOTAL FEE BALANCE DUE.

IPR2025-01572
Apple EX1002 Page 225

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**.

/mgabre/

IPR2025-01572
Apple EX1002 Page 226

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/287,597

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20=	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	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).			400			
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	1130		TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	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
15/287,597	10/06/2016	2447	0.00	RALEP041D1C1	1	1

CONFIRMATION NO. 4727

106963
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

FILING RECEIPT



Date Mailed: 10/21/2016

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Jeffrey Green, Sunnyvale, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I LLC, Tyler, TX;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 14/340,270 07/24/2014 PAT 9491199
which is a DIV of 13/309,463 12/01/2011 PAT 8793758
which claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/550,906 10/24/2011
and is a CIP of 13/237,827 09/20/2011 PAT 8832777
and is a CIP of 13/134,028 05/25/2011 PAT 8589541
and is a CIP of 13/253,013 10/04/2011 PAT 8745191
and said 13/237,827 09/20/2011
claims benefit of 61/384,456 09/20/2010
and is a CIP of 12/695,019 01/27/2010 PAT 8275830

IPR2025-01572
Apple EX1002 Page 228

which claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028 05/25/2011
claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/407,358 10/27/2010
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and said 12/694,455 01/27/2010
claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
claims benefit of 61/252,153 10/15/2009
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/134,005 05/25/2011
is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/253,013 10/04/2011
claims benefit of 61/389,547 10/04/2010
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and said 12/695,020 01/27/2010
claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 12/694,455 01/27/2010
claims benefit of 61/252,151 10/15/2009
and said 12/380,778 03/02/2009
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
and said 12/380,780 03/02/2009
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

IPR2025-01572
Apple EX1002 Page 229

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: 10/19/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/287,597**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

Preliminary Class

709

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 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

IPR2025-01572
Apple EX1002 Page 230

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 AssetsControl, 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

IPR2025-01572
Apple EX1002 Page 231

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01572
Apple EX1002 Page 232

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	not yet assigned
Serial No.:	15/287,597	Art Unit:	2447
Filed:	October 6, 2016	Conf. No.:	4727
Title:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems		

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR A CORRECTED FILING RECEIPT

Applicant respectfully requests a corrected filing receipt for the above-captioned application. Submitted with this request are:

(1) The application data sheet (ADS) filed on October 6, 2016;

(2) A copy of the Filing Receipt mailed October 21, 2016 with the requested changes noted thereon.

Applicant respectfully notes that this request is not a request to add or correct a benefit claim. Applicant is simply seeking a filing receipt that reflects the ADS that was filed on October 6, 2016.

IPR2025-01572
Apple EX1002 Page 233

CONCLUSION

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: March 1, 2017 By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: March 1, 2017 By: /Ann Taylor/
Ann Taylor

IPR2025-01572
Apple EX1002 Page 234

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.
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.

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	Woodside	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	State/Province	TX
Postal Code	75703	Country	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Jeffrey		Green	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

City	Sunnyvale	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	State/Province	TX
Postal Code	75703	Country	US

Inventor 3 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	James		Lavine	

Residence Information (Select One) ◉ US Residency Non US Residency Active US Military Service

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

City	Corte Madera	State/Province	CA	Country of Residence	US

Mailing Address of Inventor:

Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	State/Province	TX
Postal Code	75703	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	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems		
Attorney Docket Number	RALEP041D1C1	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	47	Suggested Figure for Publication (if any)	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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)
thisapplication	Continuation of	14340270	2014-07-24
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14340270	Division of	13309463	2011-12-01	8793758	2014-07-29

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61418507	2010-12-01
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61418509	2010-12-01
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61420727	2010-12-07

IPR2025-01572
Apple EX1002 Page 237

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61422565	2010-12-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61422572	2010-12-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61422574	2010-12-13
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61435564	2011-01-24
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61472606	2011-04-06
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13309463	Claims benefit of provisional	61550906	2011-10-24
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13309463	Continuation in part of	13237827	2011-09-20	8832777	2014-09-09
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13309463	Continuation in part of	13134028	2011-05-25	8589541	2013-11-19
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13309463	Continuation in part of	13253013	2011-10-04	8745191	2014-06-03

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13237827	Claims benefit of provisional	61384456	2010-09-20
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13237827	Continuation in part of	12695019	2010-01-27	8275830	2012-09-25

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695019	Claims benefit of provisional	61270353	2009-07-06
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695019	Claims benefit of provisional	61264126	2009-11-24
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61348022	2010-05-25
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61381159	2010-09-09
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61381162	2010-09-09
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61385020	2010-09-21
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61387243	2010-09-28

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61387247	2010-09-28
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13134028	Claims benefit of provisional	61407358	2010-10-27
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12694455	2010-01-27	8402111	2013-03-19

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	13134005	2011-05-25	8635335	2014-01-21

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134028	Continuation in part of	12695021	2010-01-27	8346225	2013-01-01

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12694455	Claims benefit of provisional	61264120	2009-11-24
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695021	Claims benefit of provisional	61252153	2009-10-15
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12695021	Continuation in part of	12380780	2009-03-02	8839388	2014-09-16

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134005	Continuation in part of	12380778	2009-03-02	8321526	2012-11-27

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13134005	Continuation in part of	12380780	2009-03-02	8839388	2014-09-16

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
13253013	Claims benefit of provisional	61389547	2010-10-04
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13253013	Continuation in part of	12695020	2010-01-27	8406748	2013-03-26

Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13253013	Continuation in part of	12694445	2010-01-27	8391834	2013-03-05

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695020	Claims benefit of provisional	61275208	2009-08-25
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12695020	Claims benefit of provisional	61237753	2009-08-28
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12694445	Claims benefit of provisional	61252151	2009-10-15
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380778	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)
12380778	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)
12380778	Claims benefit of provisional	61207393	2009-02-10

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
12380778	Claims benefit of provisional	61207739	2009-02-13
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
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

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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 Remove

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.

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:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Headwater Partners I LLC

Mailing Address Information For Applicant:

Address 1	1011 Pruitt Place		
Address 2			
City	Tyler	**State/Province**	TX
Country	US	Postal Code	75703
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. 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.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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)	2016-10-06
First Name	James E.	Last Name	Harris	Registration Number	40013

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	RALEP041D1C1
	Application Number	
Title of Invention	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems	

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.**

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
15/287,597	10/06/2016	2447	0.00	RALEP041D1C1	1	1

CONFIRMATION NO. 4727

106963
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

FILING RECEIPT

OC000000088816891

Date Mailed: 10/21/2016

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Jeffrey Green, Sunnyvale, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I LLC, Tyler, TX;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 14/340,270 07/24/2014 PAT 9491199
which is a DIV of 13/309,463 12/01/2011 PAT 8793758
which claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/550,906 10/24/2011
and is a CIP of 13/237,827 09/20/2011 PAT 8832777
and is a CIP of 13/134,028 05/25/2011 PAT 8589541
and is a CIP of 13/253,013 10/04/2011 PAT 8745191
and said 13/237,827 09/20/2011
claims benefit of 61/384,456 09/20/2010
and is a CIP of 12/695,019 01/27/2010 PAT 8275830

IPR2025-01572
Apple EX1002 Page 248

which claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028 05/25/2011
claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/407,358 10/27/2010
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and said 12/694,455 01/27/2010
claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
claims benefit of 61/252,153 10/15/2009
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/134,005 05/25/2011
is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/253,013 10/04/2011
claims benefit of 61/389,547 10/04/2010
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and said 12/695,020 01/27/2010
claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 12/694,455 01/27/2010 and said 12/694,445 01/27/2010
claims benefit of 61/252,151 10/15/2009
and said 12/380,778 03/02/2009
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
and said 12/380,780 03/02/2009
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

IPR2025-01572
Apple EX1002 Page 249

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: 10/19/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/287,597**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

Preliminary Class

709

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 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 AssetsControl, 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

IPR2025-01572
Apple EX1002 Page 251

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01572
Apple EX1002 Page 252

Electronic Acknowledgement Receipt	
EFS ID:	28505159
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	01-MAR-2017
Filing Date:	06-OCT-2016
Time Stamp:	16:23:19
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	Request for Corrected Filing Receipt	P041D1C1_Request.pdf	729960 8d80d50561d33055a8dccd869a48e8915bb8ee88	no	20
Warnings:					

Information:	
Total Files Size (in bytes):	729960

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
15/287,597	10/06/2016	2447	0.00	RALEP041D1C1	1	1

CONFIRMATION NO. 4727

CORRECTED FILING RECEIPT

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

OC000000089843080

Date Mailed: 03/06/2017

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Jeffrey Green, Sunnyvale, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I LLC, Tyler, TX;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 14/340,270 07/24/2014 PAT 9491199
which is a DIV of 13/309,463 12/01/2011 PAT 8793758
which claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/550,906 10/24/2011
and is a CIP of 13/237,827 09/20/2011 PAT 8832777
and is a CIP of 13/134,028 05/25/2011 PAT 8589541
and is a CIP of 13/253,013 10/04/2011 PAT 8745191
and said 13/237,827 09/20/2011
claims benefit of 61/384,456 09/20/2010
and is a CIP of 12/695,019 01/27/2010 PAT 8275830

which claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028 05/25/2011
claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/407,358 10/27/2010
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and said 12/694,455 01/27/2010
claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
claims benefit of 61/252,153 10/15/2009
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/134,005 05/25/2011
is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/253,013 10/04/2011
claims benefit of 61/389,547 10/04/2010
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and said 12/695,020 01/27/2010
claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 12/694,445 01/27/2010
claims benefit of 61/252,151 10/15/2009
and said 12/380,778 03/02/2009
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
and said 12/380,780 03/02/2009
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

IPR2025-01572
Apple EX1002 Page 256

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: 10/19/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/287,597**

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

Preliminary Class

709

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 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

IPR2025-01572
Apple EX1002 Page 257

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 AssetsControl, 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

IPR2025-01572
Apple EX1002 Page 258

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01572
Apple EX1002 Page 259

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
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1

CONFIRMATION NO. 4727

106963
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703

FORMALITIES LETTER

OC000000086616892

Date Mailed: 10/21/2016

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.)

- $ **70** basic filing fee.
- $ **400** for **51** electronically equivalent pages in excess of **100** application size fee.
- $ **70** surcharge.
- $ **300** search fee.
- $ **360** examination fee.
- $(**0**) previous unapplied payment amount.
- $ **1200** TOTAL FEE BALANCE DUE.

IPR2025-01572
Apple EX1002 Page 260

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**.

/mgabre/

IPR2025-01572
Apple EX1002 Page 261

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	not yet assigned
Serial No.:	15/287,597	Art Unit:	2447
Filed:	October 6, 2017	Conf. No.:	4727
Title:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems		

Mail Stop Amendment
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. 14/340,270 filed July 24, 2014 and U.S. Patent Application No. 13/309,463 filed December 1, 2011, of which the instant application is from the same direct family. Any foreign or non-patent references not submitted in that parent application are transmitted herewith.

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.

IPR2025-01572
Apple EX1002 Page 262

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. **50-5876**.

Respectfully submitted,

Date: March 21, 2017

By: /James E. Harris/

James E. Harris
Reg. No. 40013
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: March 21, 2017 By: /Ann Taylor/
Ann Taylor

IPR2025-01572
Apple EX1002 Page 263

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	6098878		2000-08-08	DENT et al.	
	10	6141686		2000-10-31	JACKOWSKI et al.	
	11	6148336		2000-11-14	THOMAS et al.	
	12	6198915		2001-03-06	McGREGOR et al.	
	13	6263055		2001-07-17	GARLAND et al.	
	14	6317584		2001-11-13	ABU-AMARA et al.	
	15	6418147		2002-07-09	WIEDEMAN, Robert A.	
	16	6449479		2002-09-10	SANCHEZ, Eduardo	
	17	6532235		2003-03-11	BENSON et al.	
	18	6532579		2003-03-11	SATO et al.	
	19	6539082		2003-03-25	LOWE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	6563806		2003-05-13	YANO et al.	
	21	6574321		2003-06-03	COX et al.	
	22	6574465		2003-06-03	MARSH et al.	
	23	6603969		2003-08-05	VUORISTO et al.	
	24	6639975		2003-10-28	O'NEAL et al.	
	25	6650887		2003-11-18	McGREGOR et al.	
	26	6651101		2003-11-18	GAI et al.	
	27	6658254		2003-12-02	PURDY et al.	
	28	6684244		2004-01-27	GOLDMAN et al.	
	29	6725031		2004-04-20	WATLER et al.	
	30	6765864		2004-07-20	NATARAJAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	31	6785889		2004-08-31	WILLIAMS, Peter	
	32	6829596		2004-12-07	FRAZEE, Steve	
	33	6829696		2004-12-07	BALMER et al.	
	34	6920455		2005-07-19	WESCHLER, Paul	
	35	6952428		2005-10-04	NECKA et al.	
	36	6965667		2005-11-15	TRABANDT et al.	
	37	6996076		2006-02-07	FORBES et al.	
	38	6998985		2006-02-14	REISMAN et al.	
	39	7024200		2006-04-04	McKENNA et al.	
	40	7027408		2006-04-11	NABKEL et al.	
	41	7042988		2006-05-09	JUITT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	42	7058968		2006-06-06	ROWLAND et al.	
	43	7069248		2006-06-27	HUBER, Adriano	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7142876		2006-11-28	TROSSEN et al.	
	46	7158792		2007-01-02	COOK et al.	
	47	7174174		2007-02-06	BORIS et al.	
	48	7180855		2007-02-20	LIN , Wei	
	49	7197321		2007-03-27	ERSKINE et al.	
	50	7242920		2007-07-10	MORRIS, Robert P.	
	51	7245901		2007-07-17	McGREGOR et al.	
	52	7280816		2007-10-09	FRATTI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	53	7280818		2007-10-09	CLAYTON, Steve	
	54	7289489		2007-10-30	KUNG et al.	
	55	7290283		2007-10-30	COPELAND III, John A.	
	56	7317699		2008-01-08	GODFREY et al.	
	57	7322044		2008-01-22	HRASTAR, Scott E.	
	58	7324447		2008-01-29	MORFORD, Michael Robert	
	59	7325037		2008-01-29	LAWSON, Karen L.	
	60	7349695		2008-03-25	OOMMEN et al.	
	61	7353533		2008-04-01	WRIGHT et al.	
	62	7356337		2008-04-08	FLORENCE, Shahar	
	63	7366497		2008-04-29	NAGATA, Hideaki	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	64	7373136		2008-05-13	WATLER et al.	
	65	7388950		2008-06-17	ELSEY et al.	
	66	7401338		2008-07-15	BOWEN et al.	
	67	7403763		2008-07-22	MAES, Stephane H.	
	68	7418253		2008-08-26	KAVANAH, Alan	
	69	7421004		2008-09-02	FEHER, Kamilo	
	70	7450591		2008-11-11	KORLING et al.	
	71	7450927		2008-11-11	CRESWELL et al.	
	72	7486185		2009-02-03	CULPEPPER et al.	
	73	7499537		2009-03-03	ELSEY et al.	
	74	7516219		2009-04-07	MOGHADDAM et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	75	7574731		2009-08-11	FASCENDA, Anthony C.	
	76	7580857		2009-08-25	VanFLEET et al.	
	77	7610328		2009-10-27	HAASE et al.	
	78	7617516		2009-11-10	HUSLAK et al.	
	79	7620065		2009-11-17	FALARDEAU, Eric	
	80	7620162		2009-11-17	AARON et al.	
	81	7647047		2010-01-12	MOGHADDAM et al.	
	82	7650137		2010-01-19	JOBS et al.	
	83	7668903		2010-02-23	EDWARDS et al.	
	84	7693720		2010-04-06	KENNEWICK et al.	
	85	7720505		2010-05-18	GOPI et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	86	7734784		2010-06-08	ARAUJO et al.	
	87	7747240		2010-06-29	BRISCOE et al.	
	88	7747699		2010-06-29	PRUEITT et al.	
	89	7792708		2010-09-07	ALVA, Jessi	
	90	7797204		2010-09-14	BALENT, Bruce F.	
	91	7797401		2010-09-14	STEWART et al.	
	92	7822837		2010-10-26	URBAN et al.	
	93	7848768		2010-12-07	OMORI et al.	
	94	7868778		2011-01-11	KENWRIGHT, David Norris	
	95	7873705		2011-01-18	KALISH, Dan	
	96	7882029		2011-02-01	WHITE, Craig R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	97	7929960		2011-04-19	MARTIN et al.	
	98	7937069		2011-05-03	RASSAM, Frederic	
	99	7941184		2011-05-10	PRENDERGAST et al.	
	100	7949529		2011-05-24	WEIDER et al.	
	101	7957511		2011-06-07	DRUDIS et al.	
	102	7975184		2011-07-05	GOFF et al.	
	103	7984130		2011-07-19	BOGINENI et al.	
	104	7986935		2011-07-26	D'SOUZA et al.	
	105	8005459		2011-08-23	BALSILLIE, Jim	
	106	8010080		2011-08-30	THENTHIRUPERAI et al.	
	107	8010081		2011-08-30	ROSKOWSKI, Steve	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	108	8015133		2011-09-06	WU et al.	
	109	8015234		2011-09-06	LUM et al.	
	110	8019687		2011-09-13	WANG et al.	
	111	8023425		2011-09-20	RALEIGH, Gregory G.	
	112	8095666		2012-01-10	SCHMIDT et al.	
	113	8099077		2012-01-17	CHOWDHURY et al.	
	114	8099517		2012-01-17	JIA et al.	
	115	8144591		2012-03-27	GHAI et al.	
	116	8170553		2012-05-01	BENNETT, James D.	
	117	6606744		2003-08-12	MIKURAK, Michael G.	
	118	7336960		2008-02-26	ZAVALKOVSKY et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	119	8190675		2012-05-29	TRIBBETT, David	
	120	8194549		2012-06-05	HUBER et al.	
	121	8200775		2012-06-12	MOORE, James F.	
	122	8135392		2012-03-13	MARCELLINO et al.	
	123	7953808		2011-05-31	SHARP et al.	
	124	6502131		2002-12-31	VAID, Aseem et al.	
	125	6505114		2003-01-07	LUCIANI, Sergio	
	126	6763000		2004-07-13	WALSH, Peter J.	
	127	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	128	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	129	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	130	7881199		2011-02-01	KRSTULICH, Zlatko	
	131	7886047		2011-02-08	POTLURI, Dora	
	132	7911975		2011-03-22	DROZ, Patrick et al.	
	133	8050275		2011-11-01	IYER, Jayaraman R.	
	134	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	135	8239520		2012-08-07	GRAH, Adrian	
	136	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	137	7890111		2011-02-15	Bugenhagen, Michael K.	
	138	6226277		2001-05-01	Chuah, Mooi Choo	
	139	6839340		2005-01-04	Voit, Eric A. et al.	
	140	6922562		2005-07-26	Ward, Stephen L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	141	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	142	7627314		2009-12-01	Carlson, Steven I. et al.	
	143	7792538		2010-09-07	Kozisek, Steven E.	
	144	7801523		2010-09-21	Kenderov, Stoyan	
	145	7877090		2011-01-25	Maes, Stephane H.	
	146	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	147	7948968		2011-05-24	Voit, Eric A. et al.	
	148	7970426		2011-06-28	Poe, Brian R. et al.	
	149	8185158		2012-05-22	Tamura, Motoshi et al.	
	150	8254915		2012-08-28	Kozisek, Steven E.	
	151	7418257		2008-08-26	Kim, Myong-Ju	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	152	8126123		2012-02-28	Cai, Yigang et al.	
	153	7903553		2011-03-08	Liu, Enhui	
	154	8155620		2012-04-10	Wang, Jun et al.	
	155	8238287		2012-08-07	Gopi, Paramesh et al.	
	156	7113997		2006-09-26	Jayapalan, Jay et al.	
	157	5594777		1997-01-14	Makkonen, Matti et al.	
	158	8244241		2012-08-14	Montemurro, Michael	
	159	7756534		2010-07-13	Anupam, Vinod et al.	
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	6678516		2004-01-13	Nordman, Ian et al.	
	162	6477670		2002-11-05	Ahmadvand, Nima	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	163	6038452		2000-03-14	Strawczynski, Leo et al.	
	164	8108520		2012-01-31	Ruutu, Jussi et al.	
	165	7778643		2010-08-17	Laroia, Rajiv et al.	
	166	7668176		2010-02-23	Chuah, Mooi Choo	
	167	7515608		2009-04-07	Yuan, Yuan et al.	
	168	7251218		2007-07-31	Jorgensen, Jacob W.	
	169	7002920		2006-02-21	Ayyagari, Deepak et al.	
	170	7685131		2010-03-23	Batra, Vishal Singh et al.	
	171	7283561		2007-10-16	Picher-Dempsey, Heidi	
	172	7212491		2007-05-01	Koga, Takahiro	
	173	6683853		2004-01-27	Kannas, Chris et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	174	8064896		2011-11-22	BELL, Kris M. et al.	
	175	8160015		2012-04-17	RASHID, Mohammed H. et al.	
	176	8275830		2012-09-25	Raleigh, Gregory G.	
	177	7609700		2009-10-27	Ying, Wen-Ping et al.	
	178	8255515		2012-08-28	MELMAN, David et al.	
	179	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	180	7912056		2011-03-22	BRASSEM, Wayne	
	181	7920529		2011-04-05	MAHLER, Roger et al.	
	182	8184530		2012-05-22	SWAN, Tim L. et al.	
	183	8214536		2012-07-03	ZHAO, Wen	
	184	8213363		2012-07-03	Ying, Wen-Ping et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	185	8255689		2012-08-28	KIM, Eun Ah et al.	
	186	7746854		2010-06-29	AMBE, Shekhar et al.	
	187	7068600		2006-06-27	CAIN, Joseph Bibb	
	188	6876653		2005-04-05	AMBE, Shekhar et al.	
	189	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	190	7599288		2009-10-06	COLE, Raymond E. et al.	
	191	7546629		2009-06-09	ALBERT, Anthony et al.	
	192	7747730		2010-06-29	HARLOW, James D.	
	193	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	194	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	195	7283963		2007-10-16	FITZPATRICK, John E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	196	8271049		2012-09-18	SILVER, Andrew et al.	
	197	7644151		2010-01-05	JERRIM, John et al.	
	198	8291238		2012-10-16	GINTER, Karl L. et al.	
	199	8068824		2011-11-29	SHAN, Xueshan et al.	
	200	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	201	5283904		1994-02-01	CARSON, David G. et al.	
	202	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	203	8185152		2012-05-22	GOLDNER, Alla	
	204	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	205	7873344		2011-01-18	BOWSER, Robert et al.	
	206	7856226		2010-12-21	WONG, Ellis L. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	207	7948952		2011-05-24	HURTTA, Tuija et al.	
	208	7957020		2011-06-07	MINE, Ryuta et al.	
	209	7346410		2008-03-18	UCHIYAMA, Kenji	
	210	7167078		2007-01-23	POURCHOT, Shawn C.	
	211	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	212	7970350		2011-06-28	SHEYNMAN, Arnold	
	213	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	214	8335161		2012-12-18	Foottit, Tom et al.	
	215	8315594		2012-11-20	Mauser, Edward Ronald et al.	
	216	8135388		2012-03-13	Gailloux, Michael A. et al.	
	217	6947723		2005-09-20	Gurnani, Roger et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	218	8353001		2013-01-08	Herrod, Allan	
	219	8195093		2013-06-05	Garrett, Darrin et al.	
	220	8036600		2011-10-11	Garrett, Darrin et al.	
	221	8301513		2012-10-30	Peng, Shih-Ta et al.	
	222	8230061		2012-07-24	Hassan, Amer A. et al.	
	223	8204794		2012-06-19	Peng, Shih-Ta et al.	
	224	8350700		2013-01-08	Fast, Raymond D. et al.	
	225	8204190		2012-06-19	Bang, Jung-Hee et al.	
	226	7865182		2011-01-04	Macaluso, Anthony G.	
	227	7962622		2011-06-14	Friend, John et al.	
	228	7583964		2009-09-01	Wong, Gregory A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	229	7565141		2009-07-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	240	7711848		2010-05-04	MAES, Stephane H.	
	241	6782412		2004-08-24	BROPHY, Kevin et al.	
	242	6081591		2000-06-27	SKOOG, Frederick H.	
	243	6064878		2000-05-16	DENKER, John Stewart et al.	
	244	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	245	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	246	8156206		2012-04-10	KILEY, Kevin J. et al.	
	247	8126722		2012-02-28	ROBB, Terence Alan et al.	
	248	8364089		2013-01-29	PHILLIPS, Derek	
	249	6754470		2004-06-22	Hendrickson, Keith et al.	
	250	8122128		2012-02-21	Burke, II, Robert M. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	251	8149823		2012-04-03	Turcan, Diane Brown et al.	
	252	8326359		2012-12-04	Kauffman, Donald C.	
	253	8131256		2012-03-06	MARTTI, Jyrki et al.	
	254	6381316		2002-04-30	JOYCE, Simon James et al.	
	255	7965983		2011-06-21	SWAN, Tim et al.	
	256	8284740		2012-10-09	O'CONNOR, Dennis M.	
	257	8116223		2012-02-14	TIAN, Dan et al.	
	258	6154738		2000-11-28	CALL, Charles Gainor	
	259	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	260	8306518		2012-11-06	GAILLOUX, Michael A.	
	261	8422988		2013-04-16	KESHAV, Srinivasan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	262	6035281		2000-03-07	Crosskey, James P. et al.	
	263	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	264	7760711		2010-07-20	Kung, Fen-Chung et al.	
	265	8000318		2011-08-16	Wiley, William L. et al.	
	266	8098579		2012-01-17	Ray, Amar N. et al.	
	267	8155670		2012-04-10	Fullam, Scott et al.	
	268	8374090		2013-02-12	Morrill, Robert J. et al.	
	269	7457265		2008-11-25	Julka, Vibhor et al.	
	270	7729326		2010-06-01	Sekhar, Ramesh	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7945945		2011-05-17	Graham, Richard et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	273	8059530		2011-11-15	Cole, Terry L.	
	274	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	275	8280354		2012-10-02	Smith, Christopher et al.	
	276	8331293		2012-12-11	Sood, Kapil	
	277	8019820		2011-09-13	Son, Giyeong et al.	
	278	8191116		2012-05-29	Gazzard, Daryl	
	279	6292828		2001-09-18	Williams, David L.	
	280	7043226		2006-05-09	Yamauchi, Toshiaki	
	281	7472189		2008-12-30	Mallya, Arvind R. et al.	
	282	7944948		2011-05-17	Chow, Albert T. et al.	
	283	7802724		2010-09-28	Nohr, Steven Paul	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	284	8155155		2012-04-10	Chow, Albert T. et al.	
	285	8447324		2013-05-21	Shuman, Mohammed Ataur et al.	
	286	8005009		2011-08-23	McKee, Neil et al.	
	287	7760861		2010-07-20	Croak, Marian et al.	
	288	8060463		2011-11-15	Spiegel, Joel R.	
	289	8224773		2012-07-17	Spiegel, Joel R.	
	290	8352980		2013-01-08	Howcroft, Jerald Robert	
	291	8386386		2013-02-26	Zhu, Kevin	
	292	8347362		2013-01-01	Cai, Yigang et al.	
	293	8340718		2012-12-25	Colonna, Massimo et al.	
	294	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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	295	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	296	8279864		2012-10-02	Wood, Daniel M.	
	297	8271045		2012-09-18	Parolkar, Satish et al.	
	298	8233883		2012-07-31	De Froment, Eric	
	299	8224382		2012-07-17	Bultman, Michael J.	
	300	8184590		2012-05-22	Rosenblatt, Ariel	

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	1	1463238	EP		2004-09-29	Alcatel		
	2	1739518	EP		2007-01-03	Research In Motion Limited		
	3	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		
	4	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		
	5	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		
	6	2003014891	WO		2003-02-20	The Boeing Company		
	7	2003058880	WO		2003-07-17	Telia AB		
	8	2004028070	WO		2004-04-01	Credant Technologies, Inc.		
	9	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		
	10	2004095753	WO		2004-11-04	Motorola Inc.		
	11	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	12	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		
	13	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		
	14	2006077481	WO		2006-07-27	TrueContext Corporation		
	15	2006130960	WO		2006-12-14	Mobidia, Inc.		
	16	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		
	17	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		
	18	2007018363	WO		2007-02-15	Upresto, Inc.		
	19	2007053848	WO		2007-05-10	Mobile Armor, LLC		
	20	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		
	21	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		
	22	2008017837	WO		2008-02-14	Symbian Software Limited		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	23	2008051379	WO		2008-05-02	Verizon Services Corp.		
	24	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		
	25	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		
	26	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		
	27	2008099802	WO		2008-08-21	NEC Corporation		
	28	2010088413	WO		2010-08-05	Headwater Partners I LLC		
	29	2006120558	WO		2006-11-16	Nokia Corp.		
	30	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		
	31	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		
	32	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		
	33	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	34	2005008995	WO		2005-01-27	Starhub Ltd.		
	35	1998058505	WO		1998-12-23	Sonera Oy		
	36	2007097786	WO		2007-08-30	Sony Ericsson Mobile Communications AB		

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.	T5
	1	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	
	2	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	
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	7	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	
	8	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	
	9	European Commission, "Data Roaming Tariffs - Transparency Measures," [online] retrieved from http://web.archive.org/web/20081220232754/http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm, December 20, 2008 [retrieved May 16, 2012]	
	10	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	
	11	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	
	12	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	
	13	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	
	14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	
	15	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	
	16	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	
	17	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	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	
	25	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)	
	26	Ruckus Wireless – White Paper; "Smarter Wi-Fi for Mobile Operator Infrastructures" 2010	
	27	Accuris Networks, "The Business Value of Mobile Data Offload – a White Paper", 2010	
	28	Wireless Broadband Alliance, "WISPr 2.0, 08 April, 2010"; Doc. Ref. No.: WBA/RM/WISPr, Version 01.00	

IPR2025-01572
Apple EX1002 Page 297

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	29	THURSTON, Richard, "WISPr 2.0 Boosts Roaming Between 3G and Wi-Fi"; June 23, 2010; Web page from zdnet.com; Zdnet.com/wispr-2-0-boosts-roaming-between-3g-and-wi-fi-3040089325/	
	30	Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group, "Hotspot 2.0 (Release 1) Technical Specification – Version 1.0.0"; 2012	
	31	Wi-Fi Alliance Hotspot 2.0 Technical Task Group, "Wi-Fi Certified Passpoint™ (Release 1) Deployment Guidelines – Version 1.0 – October 2012"	

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

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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2017-03-21
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	8174970		2012-05-08	Adamczyk, Maria et al.	
	2	8165576		2012-04-24	Raju, Vishwanath et al.	
	3	8073721		2011-12-06	Lewis, Lundy	
	4	8032899		2011-10-04	Archer, Charles J. et al.	
	5	7974624		2011-07-05	Gallagher, Michael D. et al.	
	6	7907970		2011-03-15	Park, Vincent D. et al.	
	7	7778176		2010-08-17	Morford, Michael Robert	
	8	7725570		2010-05-25	Lewis, Lundy	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	7634388		2009-12-15	Archer, Charles J. et al.	
	10	7633438		2009-12-15	Tysowski, Piotr Konrad	
	11	7593417		2009-09-22	Wang, James et al.	
	12	7551922		2009-06-23	Roskowski, Steve et al.	
	13	7545782		2009-06-09	Rayment, Stephen G. et al.	
	14	7039037		2006-05-02	Wang, Jiwei R. et al.	
	15	6928280		2005-08-09	Xanthos, James et al.	
	16	6765925		2004-07-20	Sawyer, Wilson et al.	
	17	5889477		1999-03-30	Fastenrath, Ulrich	
	18	8332517		2012-12-11	Russell, Jesse E.	
	19	8315718		2012-11-20	Caffrey, Paul Oliver et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	8447980		2013-05-21	Godfrey, James A. et al.	
	21	8429403		2013-04-23	Moret, Eric et al.	
	22	8411587		2013-04-02	Curtis, William et al.	
	23	8396929		2013-03-12	Helfman, Nadav et al.	
	24	8363658		2013-01-29	Delker, Jason R. et al.	
	25	8265004		2012-09-11	Toutonghi, Michael J.	
	26	8233895		2012-07-31	Tysowski, Piotr Konrad	
	27	7685254		2010-03-23	Pandya, Ashish A.	
	28	7181017		2007-02-20	Nagel, Robert H. et al.	
	29	6965872		2005-11-15	Grdina, Jerome M.	
	30	8406427		2013-03-26	Chand, Naresh et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	31	8429409		2013-04-23	Wall, Jonathan et al.	
	32	8402540		2013-03-19	Kapoor, Harsh et al.	
	33	8135657		2012-03-13	Kapoor, Harsh et al.	
	34	8271992		2012-09-18	Chatley, Scott P. et al.	
	35	8315999		2012-11-20	Chatley, Scott P. et al.	
	36	8332375		2012-12-11	Chatley, Scott P. et al.	
	37	8468337		2013-06-18	Gaur, Santosh P. et al.	
	38	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	39	8352630		2013-01-08	Hart, Justin Scott	
	40	6640097		2003-10-28	Corrigan, Louis et al.	
	41	7039713		2006-05-02	Van Gunter, David et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	42	5915008		1999-06-22	Dulman, Scott	
	43	8126476		2012-02-28	Vardi, Yosef et al.	
	44	8000276		2011-08-16	Scherzer, Shimon et al.	
	45	8358638		2013-01-22	Scherzer, Tamir et al.	
	46	8356336		2013-01-15	Johnston, Keith et al.	
	47	8307067		2012-11-06	Ryan, Nicholas M.	
	48	7286848		2007-10-23	Vireday, Richard P. et al.	
	49	7313237		2007-12-25	Bahl, Paramvir et al.	
	50	7444669		2008-10-28	Bahl, Paramvir et al.	
	51	7548976		2009-06-16	Bahl, Paramvir et al.	
	52	8027339		2011-09-27	Short, Joel E. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	53	8095112		2012-01-10	Chow, Richard et al.	
	54	8369274		2013-02-05	Sawai, Ryo	
	55	7881697		2011-02-01	Baker, Matthew Donald et al.	
	56	7899438		2011-03-01	Baker, Matthew Donald et al.	
	57	7945238		2011-05-17	Baker, Matthew Donald et al.	
	58	8078140		2011-12-13	Baker, Matthew Donald et al.	
	59	8285249		2012-10-09	Baker, Matthew Donald et al.	
	60	7493659		2009-02-17	Wu, Handong et al.	
	61	7801985		2010-09-21	Pitkow, Jim et al.	
	62	8242959		2012-08-14	Mia, Rashidus S. et al.	
	63	8326319		2012-12-04	Davis, Richard W.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	64	8019886		2011-09-13	Harrang, Jeffrey Paul et al.	
	65	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	
	66	7139569		2006-11-21	Kato, Akira	
	67	7529204		2009-05-05	Bourlas, Yair et al.	
	68	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	69	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	70	8032409		2011-10-04	Mikurak, Michael G.	
	71	8045973		2011-10-25	Chambers, Michael D.	
	72	8116781		2012-02-14	Chen, Xixian et al.	
	73	8126396		2012-02-28	Bennett, James D.	
	74	8351898		2013-01-08	Raleigh, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	75	5630159		1997-05-13	Zancho, William F.	
	76	5633484		1997-05-27	Zancho, William F. et al.	
	77	5814798		1998-09-29	Zancho, William F.	
	78	7039403		2006-05-02	Wong, Gregory A.	
	79	7583964		2009-09-01	Wong, Gregory A.	
	80	7593730		2009-09-22	Khandelwal, Deepak et al.	
	81	7948953		2011-05-24	Melkote, Keerti G. et al.	
	82	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	83	8270972		2012-09-18	Otting, Marcia J. et al.	
	84	7929959		2011-04-19	DeAtley, Dallas et al.	
	85	7478420		2009-01-13	Wright, Michael et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	86	7502672		2009-03-10	Kolls, H. Brock	
	87	7756757		2010-07-13	Oakes III, Charles Lee	
	88	7930446		2011-04-19	Kesselman, Alex et al.	
	89	8078163		2011-12-13	Lemond, Eric et al.	
	90	8068829		2011-11-29	Lemond, Eric et al.	
	91	8086497		2011-12-27	Oakes III, Charles Lee	
	92	8166040		2012-04-24	Brindisi, Richard G. et al.	
	93	6934249		2005-08-23	Bertin, Olivier et al.	
	94	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	95	8447607		2013-05-21	Weider, Chris et al.	
	96	8504729		2013-08-06	Pezzutti, David A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	97	8495227		2013-07-23	Kaminsky, David L. et al.	
	98	8472371		2013-06-25	Bari, Farooq et al.	
	99	8134954		2012-03-13	Godfrey, James A. et al.	
	100	7535880		2009-05-19	Hinman, Brian L. et al.	
	101	7499438		2009-03-03	Hinman, Brian L. et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	104	6654814		2003-11-25	Britton, Kathryn H. et al.	
	105	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	106	8325638		2012-12-04	Jin, Haipeng et al.	
	107	8116749		2012-02-14	Proctor Jr., James Arthur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	108	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	109	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	110	8150431		2012-04-03	Wolovitz, Lionel et al.	
	111	8483135		2013-07-09	Cai, Yigang et al.	
	112	6104700		2000-08-15	Haddock, Stephen R. et al.	
	113	8185127		2012-05-22	Cai, Zheng et al.	
	114	8521110		2013-08-27	Rofougaran, Ahmadreza	
	115	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	117	7546460		2009-06-09	Maes, Stephane H.	
	118	7921463		2011-04-05	Sood, Kapil et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	119	7940751		2011-05-10	Hansen, Christopher J.	
	120	8122249		2012-02-21	Falk, Rainer et al.	
	121	8495360		2013-07-23	Falk, Rainer et al.	
	122	8520589		2013-08-27	Bhatt, Yogesh et al.	
	123	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	124	8379847		2013-02-19	Bell, Robert H. et al.	
	125	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	126	8296404		2012-10-23	McDysan, Dave et al.	
	127	8195163		2012-06-05	Gisby, Doug et al.	
	128	8437734		2013-05-07	Ray, Amar N. et al.	
	129	8280351		2012-10-02	Ahmed, Shahid et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	130	7460837		2008-12-02	Diener, Neil R.	
	131	7653394		2010-01-26	McMillin, Brian K.	
	132	8130793		2012-03-06	Edwards, Stephen K. et al.	
	133	8509082		2013-08-13	Heinz, John M. et al.	
	134	8526329		2013-09-03	Mahany, Ronald L. et al.	
	135	5983270		1999-11-09	Abraham, Dalen M. et al.	
	136	6598034		2003-07-22	Kloth, Axel K.	
	137	7032072		2006-04-18	Quinn, Michael J. et al.	
	138	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	139	7742406		2010-06-22	Muppala, Suresh	
	140	7953877		2011-05-31	Vemula, Narendra et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	141	7957381		2011-06-07	Clermidy, Fabien et al.	
	142	8031601		2011-10-04	Feroz, Azeem et al.	
	143	8255534		2012-08-28	Assadzadeh, Alireza	
	144	8489720		2013-07-16	Morford, Michael Robert et al.	
	145	7774323		2010-08-10	Helfman, Nadav	
	146	7043268		2006-05-09	Yukie, Satoru et al.	
	147	8391262		2013-03-05	Maki, Lasse et al.	
	148	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	149	8166554		2012-04-24	John, Pramod	
	150	7697540		2010-04-13	Haddad, Reda et al.	
	151	6748195		2004-06-08	Phillips, W. Garland	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	152	8583499		2013-11-12	De Judicibus, Dario et al.	
	153	8352360		2013-01-08	De Judicibus, Dario et al.	
	154	8463232		2013-06-11	Tuli, Amol et al.	
	155	7958029		2011-06-07	Bobich, Thomas et al.	
	156	7540408		2009-06-02	Levine, Judah Joseph et al.	
	157	7826427		2010-11-02	Sood, Kapil et al.	
	158	8185088		2012-05-22	Klein, Robert S. et al.	
	159	8548428		2013-10-01	Raleigh, Gregory G.	
	160	8483694		2013-07-09	Lewis, Allan D. et al.	
	161	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	162	8452858		2013-05-28	Wu, John et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	163	7610396		2009-10-27	Taglienti, Claudio et al.	
	164	7984511		2011-07-19	Kocher, Paul Carl et al.	
	165	7987510		2011-07-26	Kocher, Paul C. et al.	
	166	8571993		2013-10-29	Kocher, Paul C. et al.	
	167	8543265		2013-09-24	Ekhaguere, David E. et al.	
	168	8385975		2013-02-26	Forutanpour, Babak	
	169	6873988		2005-03-29	Hermann, Conrad K. et al.	
	170	7013469		2006-03-14	Smith, Adam W. et al.	
	171	7203169		2007-04-10	Okholm, Jon Eric et al.	
	172	7286834		2007-10-23	Walter, Edward	
	173	7555757		2009-06-30	Smith, Adam W. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	174	7574509		2009-08-11	Nixon, Mark J. et al.	
	175	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	176	7940685		2011-05-10	Breslau, Lee Michel et al.	
	177	8196199		2012-06-05	Hrastar, Scott E. et al.	
	178	8204505		2012-06-19	Jin, Haipeng et al.	
	179	8228818		2012-07-24	Chase, Christopher J. et al.	
	180	8320244		2012-11-27	Muqattash, Alaa et al.	
	181	8411691		2013-04-02	Aggarwal, Rahul	
	182	8461958		2013-06-11	Saenz, Jorge E. et al.	
	183	8484327		2013-07-09	Werner, Eran et al.	
	184	8522039		2013-08-27	Hyndman, Arn et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	185	8544105		2013-09-24	Mclean, Ivan H. et al.	
	186	8571474		2013-10-29	Chavez, Timothy R. et al.	
	187	8194572		2012-06-05	Horvath, Robert et al.	
	188	8516552		2013-08-20	Raleigh, Gregory G.	
	189	8441955		2013-05-14	Wilkinson, Robert Todd et al.	
	190	5774532		1998-06-30	Gottlieb, Louis G. et al.	
	191	8095124		2012-01-10	Balia, Hinal K.	
	192	7797060		2010-09-14	Grgic, Richard J. et al.	
	193	7930327		2011-04-19	Craft, David Jones et al.	
	194	8264965		2012-09-11	Dolganow, Andrew et a.	
	195	8626115		2014-01-07	Raleigh, Gregory G. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	196	6885997		2005-04-26	Roberts, David T.	
	197	8229394		2012-07-24	Karlberg, Johan	
	198	8495700		2013-07-23	Shahbazi, Majid	
	199	8548427		2013-10-01	Chow, Paulo S.T. et al.	
	200	8572117		2013-10-29	Rappaport, Theodore S.	
	201	8589955		2013-11-19	Roundtree, Brian et al.	
	202	8660853		2014-02-25	Robb, Terence A. et al.	
	203	8601125		2013-12-03	Huang, Shibi et al	
	204	8046449		2011-10-25	Yoshiuchi, Hideya	
	205	8635164		2014-01-21	Rosenhaft, Matthew et al.	
	206	8566236		2013-10-22	Busch, James David	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	207	8528068		2013-09-03	Weglein, Joseph et al.	
	208	8442015		2013-05-14	Behzad, Arya et al	
	209	7853255		2010-12-14	Karaoguz, Jeyhan et al	
	210	7720464		2010-05-18	Batta, Puneet	
	211	8300575		2012-10-30	Willars, Per	
	212	8666395		2014-03-04	Silver, Andrew	
	213	8315593		2012-11-20	Gallant, John K. et al.	
	214	8180881		2012-05-15	Seo, Kyoung-Il et al.	
	215	7539132		2009-05-26	Werner, Carl E. et al.	
	216	8589541		2013-11-19	Raleigh, Gregory G. et al.	
	217	7805606		2010-09-28	Birger, Chet et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	218	8347378		2013-01-01	Merkin, Aaron E. et al.	
	219	8391834		2013-03-05	Raleigh, Gregory G.	
	220	6185576		2001-02-06	McIntosh, Lowrie	
	221	8175574		2012-05-08	Panda, Biswaranjan et al.	
	222	8375128		2013-02-12	Tofighbakhsh, Mostafa et al.	
	223	8527410		2013-09-03	Markki, Outi et al.	
	224	7320029		2008-01-15	Rinne, Janne Petri et al.	
	225	8275415		2012-09-25	Huslak, Nicholas S.	
	226	8539561		2013-09-17	Gupta, Akhilesh et al.	
	227	8554876		2013-10-08	Winsor, Gerald W.	
	228	8191124		2012-05-29	Wynn, Simon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	229	7805140		2010-09-28	Friday, Robert J. et al.	
	230	8605691		2013-12-10	Soomro, Amjad et al.	
	231	8655357		2014-02-18	Gazzard, Daryl Robert et al.	
	232	8706863		2014-04-22	Fadell, Anthony	
	233	6640334		2003-10-28	Rasmussen, John H.	
	234	7668612		2010-02-23	Okkonen, Harri	
	235	5325532		1994-06-28	Crosswy, Wm. Caldwell et al.	
	236	7614051		2009-11-03	Glaum, Jeffrey D. et al.	
	237	5131020		1992-07-14	Liebesny, John P. et al.	
	238	8223741		2012-07-17	Bartlett, Roger Danforth et al.	
	239	8396458		2013-03-12	Raleigh, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	240	8370483		2013-02-05	Choong et al.	
	241	8670334		2014-03-11	Keohane et al.	
	242	8693323		2014-04-08	McDysan, David E.	
	243	7409447		2008-08-05	Assadzadeh, Alireza	
	244	8725899		2014-05-13	Short, Joel et al.	
	245	8676925		2014-03-18	Liu, Jiawei et al.	
	246	8645518		2014-02-04	David, Scott L.	
	247	7756056		2010-07-13	Kim et al	
	248	8131281		2012-03-06	Hildner et al.	
	249	8160598		2012-04-17	Savoor, Raghvendra	
	250	8375136		2013-02-12	Roman et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	251	6119933		2000-09-19	Wong et al.	
	252	8694772		2014-04-08	Kao et al.	
	253	8719423		2014-05-06	Wyld, Jeremy	
	254	8347104		2013-01-01	Pathiyal, Krishna K.	
	255	7149229		2006-12-12	Leung, Kent K.	
	256	7242668		2007-07-10	Kan, Chao et al.	
	257	8095640		2012-01-10	Guingo, Pierrick et al.	
	258	8705361		2014-04-22	Venkataraman, Ramesh et al.	
	259	8780857		2014-07-15	Balasubramanian, Srinivasan et al.	
	260	8811991		2014-08-19	Jain, Nikhil et al.	
	261	7809351		2010-10-05	Panda et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	262	8346210		2013-01-01	Balsan, Damien et al.	
	263	8355696		2013-01-15	Olding et al.	
	264	8488597		2013-07-16	Nie et al.	
	265	6438575		2002-08-20	Khan et al.	
	266	7222304		2007-05-22	Beaton et al.	
	267	7561899		2009-07-14	Lee, Changseok	
	268	8200200		2012-06-12	Belser et al.	
	269	8229914		2012-07-24	Ramer et al.	
	270	8522249		2013-08-27	Beaule, Stephane	
	271	8701015		2014-04-15	Bonnat, Pierre	
	272	6697821		2004-02-24	Ziff et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	273	6763226		2004-07-13	McZeal Jr., Alfred	
	274	6982733		2006-01-03	McNally et al.	
	275	6983370		2006-01-03	Eaton, et al.	
	276	7318111		2008-01-08	Zhao, Wen	
	277	8064418		2011-11-22	Maki, Lasse	
	278	8249601		2012-08-21	Emberson et al.	
	279	8514927		2013-08-20	Sundararajan et al.	
	280	8634425		2014-01-21	Gorti et al.	
	281	8825109		2014-09-02	Montemurro et al.	
	282	9014973		2015-04-21	Ruckart, John	
	283	8977284		2015-03-10	Reed, Mark J.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	284	8930238		2015-01-06	Coffman et al.	
	285	8880047		2014-11-04	Konicek et al.	
	286	8739035		2014-05-27	Trethewey, Jim	
	287	8571598		2013-07-16	Valavi, John J.	
	288	8489110		2013-07-16	Frank et al.	
	289	8406736		2013-03-26	Das et al.	
	290	8259692		2012-09-04	Bajko, Gabor	
	291	8233433		2012-07-31	Kalhan, Amit	
	292	8155666		2012-04-10	Alizadeh-Shabdiz, Farshid	
	293	8103285		2012-01-24	Kalhan, Amit	
	294	7936736		2011-05-03	Proctor Jr., James Arthur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	295	7925778		2011-04-12	Wijnands et al.	
	296	7760137		2010-07-20	Martucci et al.	
	297	7684370		2010-03-23	Kezys, Vytautas Robertas	
	298	7084775		2006-08-01	Smith, Michael R.	
	299	6578076		2003-06-10	Putzolu, David Matthew	
	300	7133695		2006-11-07	Beyda, William J.	

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		
	5	1802839A	CN		2006-07-12	Motorola Inc.		
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		
	7	101123553A	CN		2007-09-11	SouTheast University		
	8	1937511A	CN		2007-03-28	ZTE		
	9	2466831A1	EP		2012-06-20	Openet Telecom Ltd./ McNamee et al.		
	10	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		
	11	2007133844	WO		2007-11-22	Camiant, Inc.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	12	2011149532 A1	WO		2011-12-01	Raleigh, Gregory G. et al.		
	13	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		
	14	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		
	15	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		
	16	101815275A	CN		2010-08-25	Yang, Liu		

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.	T5
	1	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	
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	
	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	"Prevent iCloud Documents & Data from using your data plan," October 26, 2011; CNET webarchive, by Jason Ciprian	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	5	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 11)," 3GPP Standard; 3GPP TS 23.203 v11.6.0; Sophia Antipolis, France; pp. 1-177; June 2012	
	6	"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	
	7	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	

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

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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2017-03-21
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	7260382		2007-08-21	Lamb et al.	
	2	7685530		2010-03-23	Sherrard et al.	
	3	7937450		2011-05-03	Janik, Craig M.	
	4	8019846		2011-09-13	Roelens et al.	
	5	8050705		2011-11-01	Sicher et al.	
	6	8086791		2011-12-27	Caulkins, Jason	
	7	7627872		2009-12-01	Hebeler et al.	
	8	8532610		2013-09-10	Manning Cassett et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	8631428		2014-01-14	Scott et al.	
	10	8804517		2014-08-12	Oerton, Kevin John	
	11	8949597		2015-02-03	Reeves et al.	
	12	8831561		2014-09-09	Sutaria et al.	
	13	8010082		2011-08-30	Sutaria et al.	
	14	7271765		2007-09-18	Stilp et al.	
	15	7843843		2010-11-30	Papp III et al.	
	16	8495181		2013-07-23	Venkatraman et al.	
	17	9049010		2015-06-02	Jueneman et al.	
	18	8174378		2012-05-08	Richman et al.	
	19	6757717		2004-06-29	Goldstein, Leonid	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	7007295		2006-02-28	Rose et al.	
	21	8208788		2012-06-26	Ando et al.	
	22	8326828		2012-12-04	Zhou et al.	
	23	8761711		2014-06-24	Grignani et al.	
	24	7222190		2007-05-22	Klinker, Eric et al.	
	25	8713535		2014-04-29	Malhotra et al.	
	26	5572528		1996-11-05	Shuen, Pauline	
	27	5754953		1998-05-19	Briancon et al.	
	28	6628934		2003-09-30	Rosenberg et al.	
	29	6662014		2003-12-09	Walsh, Patrick Jay	
	30	6901440		2005-05-31	Bimm et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	31	6970692		2005-11-29	Tysor, Arthur James	
	32	7203752		2007-04-10	Rice et al.	
	33	7224968		2007-05-29	Dobson et al.	
	34	7379731		2008-05-27	Natsuno et al.	
	35	7457870		2008-11-25	Lownsbrough et al.	
	36	7515926		2009-04-07	Bu et al.	
	37	7536695		2009-05-19	Alam et al.	
	38	7586871		2009-09-08	Hamilton et al.	
	39	7752330		2010-07-06	Olsen et al.	
	40	7792257		2010-09-07	Vanier et al.	
	41	7801783		2010-09-21	Kende et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	42	7865187		2011-01-04	Ramer et al.	
	43	7933274		2011-04-26	Verma et al.	
	44	8005726		2011-08-23	Bao, Yulin	
	45	8050690		2011-11-01	Neeraj, Chawla	
	46	8086398		2011-12-27	Sanchez et al.	
	47	8107953		2012-01-31	Zimmerman et al.	
	48	8112435		2012-02-07	Epstein et al.	
	49	8195661		2012-06-05	Kalavade, Asawaree	
	50	8200163		2012-06-12	Hoffman, George E.	
	51	8200818		2012-06-12	Freund et al.	
	52	8254880		2012-08-28	Aaltonen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	53	8270955		2012-09-18	Ramer et al.	
	54	8331223		2012-12-11	Hill et al.	
	55	8358975		2013-01-22	Bahl et al.	
	56	8533775		2013-09-10	Alcorn et al.	
	57	8538394		2013-09-17	Zimmerman et al.	
	58	8538458		2013-09-17	Haney, Richard D.	
	59	8565746		2013-10-22	Hoffman, George E.	
	60	8571501		2013-10-29	Miller et al.	
	61	8644702		2014-02-04	Kalajan, Kevin E.	
	62	8713641		2014-04-29	Pagan et al.	
	63	8730842		2014-05-20	Collins et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	64	8732808		2014-05-20	Sewall et al.	
	65	6445777		2002-09-03	Clark, Curtis	
	66	7039027		2006-05-02	Bridgelall, Raj	
	67	7990049		2011-08-02	Shioya, Shunsuke	
	68	8180886		2012-05-15	Overcash et al.	
	69	8339991		2012-12-25	Biswas et al.	
	70	8630314		2014-01-14	York, Frederick John	
	71	8868725		2014-10-21	Samba, Augustine S.	
	72	7149521		2006-12-12	Sundar et al.	
	73	7200112		2007-04-03	Sundar et al.	
	74	7395244		2008-07-01	Kingsford, Bryan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	75	7411930		2008-08-12	Montojo, Juan et al.	
	76	7508799		2009-03-24	Sumner et al.	
	77	7554983		2009-06-30	Muppala, Suresh	
	78	7564799		2009-07-21	Holland et al.	
	79	7849477		2010-12-07	Cristofalo et al.	
	80	7987496		2011-07-26	Bryce et al.	
	81	8503455		2013-08-06	Heikens, Heico	
	82	RE44412		2013-08-06	Naqvi et al.	
	83	8484568		2013-07-09	Rados et al.	
	84	5974439		1999-10-26	Bollella, Gregory	
	85	6882718		2005-04-19	Smith, Benjamin V.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	86	7058022		2006-06-06	Carolan et al.	
	87	7017189		2006-03-21	DeMello et al.	
	88	7266371		2007-09-04	Amin et al.	
	89	8190122		2012-05-29	Alexander et al.	
	90	9002342		2015-04-07	Tenhunen et al.	
	91	8385964		2013-02-26	Haney, Richard D.	
	92	8504032		2013-08-06	Lott et al.	
	93	7366654		2008-04-29	Moore, Robert C.	
	94	7391724		2008-06-24	Alakoski et al.	
	95	7978686		2011-07-12	Goyal et al.	
	96	8644813		2014-02-04	Gailloux et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	97	6393014		2002-05-21	Daly et al.	
	98	6397259		2002-05-28	Lincke et al.	
	99	7047276		2006-05-16	Liu et al.	
	100	7627767		2009-12-01	Sherman et al.	
	101	7849161		2010-12-07	Koch et al.	
	102	7894431		2011-02-22	Goring et al.	
	103	8073427		2011-12-06	Koch et al.	
	104	8522337		2013-08-27	Adusumilli et al.	
	105	8527662		2013-09-03	Biswas et al.	
	106	8572256		2013-10-29	Babbar, Uppinder Singh	
	107	8966018		2015-02-24	Bugwadia et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	108	7162237		2007-01-09	Silver et al.	
	109	7454191		2008-11-18	Dawson et al.	
	110	7817615		2010-10-19	Breau et al.	
	111	7844034		2010-11-30	Oh et al.	
	112	7899039		2011-03-01	Andreasen et al.	
	113	8104080		2012-01-24	Burns et al.	
	114	8150394		2012-04-03	Bianconi et al.	
	115	8667542		2014-03-04	Bertz et al.	
	116	8793304		2014-07-29	Lu et al.	
	117	8948726		2015-02-03	Smith et al.	
	118	7860088		2010-12-28	Lioy, Marcello	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	119	8812525		2014-08-19	Taylor III, Buford Leonard	
	120	8504690		2013-08-06	Shah et al.	
	121	8407763		2013-03-26	Weller et al.	
	122	8131840		2012-03-06	Denker, Richard E.	
	123	7676673		2010-03-09	Weller et al.	
	124	7512128		2009-03-31	DiMambro et al.	
	125	7248570		2007-07-24	Bahl et al.	
	126	7024460		2006-04-04	Koopmas et al.	
	127	6748437		2004-06-08	Mankude et al.	
	128	6735206		2004-05-11	Oki et al.	
	129	6058434		2000-05-02	Wilt et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	130	8032168		2011-10-04	Ikaheimo, Jorma	
	131	7966405		2011-06-21	Sundaresan et al.	
	132	7889384		2011-02-15	Armentrout et al.	
	133	6125391		2000-09-26	Meltzer et al.	
	134	6038540		2000-03-14	Krist et al.	
	135	8504687		2013-08-06	Maffione et al.	
	136	8863111		2014-10-14	Selitser et al.	
	137	8972537		2015-03-03	Bastian et al.	
	138	9176913		2015-11-03	Millet et al.	
	139	7043225		2006-05-09	Patel et al.	
	140	6725256		2004-04-20	Albal et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	141	6751296		2004-06-15	Albal et al.	
	142	6934751		2005-08-23	Jayapalan et al.	
	143	7174156		2007-02-06	Mangal, Manish	
	144	7636626		2009-12-22	Oesterling et al.	
	145	7720206		2010-05-18	Devolites et al.	
	146	8180333		2012-05-15	Wells et al.	
	147	8340678		2012-12-25	Pandey, Vinod	
	148	8005913		2011-08-23	Carlander, Carrie	
	149	6792461		2004-09-14	Hericourt, Olivier	
	150	7027055		2006-04-11	Anderson et al	
	151	8160056		2012-04-17	Van der Merwe et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	152	5633868		1997-05-27	Baldwin et al.	
	153	7680086		2010-03-16	Eglin, Matthew George	
	154	7765294		2010-07-27	Edwards et al.	
	155	7843831		2010-11-30	Morrill et al.	
	156	8131858		2012-03-06	Agulnik et al.	
	157	8223655		2012-07-17	Heinz et al.	
	158	8385199		2013-02-26	Coward et al.	
	159	8520595		2013-08-27	Yadav et al.	
	160	9135037		2015-09-15	Petrescu-Prahova et al.	
	161	6061571		2000-05-09	Tamura, Hideo	
	162	6157636		2000-12-05	Voit et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	163	7110753		2006-09-19	Campen, Kenneth Brian	
	164	8523547		2013-09-03	Pekrul, Merton W.	
	165	8875042		2014-10-28	Lejeune et al.	
	166	9177455		2015-11-03	Remer, David M.	
	167	8315198		2012-11-20	Corneille et al.	
	168	9172553		2015-10-27	Dawes et al.	
	169	8621056		2013-12-31	Coussemaeker et al.	
	170	7770785		2010-08-10	Jha et al.	
	171	7817983		2010-10-19	Cassett et al.	
	172	8600895		2013-12-03	Felsher, David Paul	
	173	6535855		2003-03-18	Cahill et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	174	6654786		2003-11-25	Fox et al.	
	175	7272660		2007-09-18	Powers et al.	
	176	8065365		2011-11-22	Saxena et al.	
	177	8085808		2011-12-27	Brusca et al.	
	178	8325906		2012-12-04	Fullarton et al.	
	179	8340628		2012-12-25	Taylor et al.	
	180	8448015		2013-05-21	Gerhart, David	
	181	8675852		2014-03-18	Maes, Stephane H.	
	182	8971912		2015-03-03	Chou et al.	
	183	8151205		2012-04-03	Follmann et al.	
	184	7133386		2006-11-07	Holur et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	185	8744339		2014-06-03	Halfmann et al.	
	186	8811338		2014-08-19	Jin et al.	
	187	8908516		2014-12-09	Tzamaloukas et al.	
	188	9030934		2015-05-12	Shah et al.	
	189	7440433		2008-10-21	Rink et al.	
	190	8191106		2012-05-29	Choyi et al.	
	191	6947985		2005-09-20	Hegli et al.	
	192	8195153		2012-06-05	Frencel et al.	
	193	8505073		2013-08-06	Taglienti et al.	
	194	8898748		2014-11-25	Burks et al.	
	195	9282460		2016-03-08	Souissi, Slim Salah	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	196	8995952		2015-03-31	Baker et al.	
	197	8971841		2015-03-03	Menezes et al.	
	198	8538421		2013-09-17	Brisebois et al.	
	199	8503358		2013-08-06	Hanson et al.	
	200	8271025		2012-09-18	Brisebois et al.	
	201	7661124		2010-02-09	Ramanathan et al.	
	202	6141565		2000-10-31	Feurerstein et al.	
	203	6690918		2004-02-10	Evans et al.	
	204	7657920		2010-02-02	Arseneau et al.	
	205	7724716		2010-05-25	Fadell, Anthony M.	
	206	8320902		2012-11-27	Moring et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	207	8837322		2014-09-16	Venkataramanan et al.	
	208	9325737		2016-04-26	Gutowski et al.	
	209	9344557		2016-05-17	Gruchala et al.	
	210	8731519		2014-05-20	Flynn et al.	
	211	8363799		2013-01-29	Gruchala et al.	
	212	6510152		2003-01-21	Gerszberg et al.	
	213	6542500		2003-04-01	Gerszberg et al.	
	214	6546016		2003-04-08	Gerszberg et al.	
	215	6570974		2003-05-27	Gerszberg et al.	
	216	7082422		2006-07-25	Zirngibl et al.	
	217	7369848		2008-05-06	Jiang, Yue Jun	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	218	7577431		2009-08-18	Jiang, Yue Jun	
	219	7664494		2010-02-16	Jiang, Yue Jun	
	220	7873001		2011-01-18	Silver, Andrew	
	221	8219134		2012-07-10	Maharajh et al.	
	222	8291439		2012-10-16	Jethi et al.	
	223	9367680		2016-06-14	Mahaffey et al.	
	224	8670752		2014-03-11	Fan et al.	
	225	9032427		2015-05-12	Gallant et al.	
	226	9173090		2015-10-27	Tuchman et al.	
	227	9367680		2016-06-14	Mahaffey et al.	
	228	6636721		2003-10-21	Threadgill et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	229	7979069		2011-07-12	Hupp et al.	
	230	8145194		2012-03-27	Yoshikawa et al.	
	231	8380247		2013-02-19	Engstrom, G. Eric	
	232	8494559		2013-07-23	Malmi, Robert A.	
	233	8719397		2014-05-06	Levi et al.	
	234	8838752		2014-09-16	Lor et al.	
	235	6959393		2005-10-25	Hollis et al.	
	236	7177919		2007-02-13	Truong et al.	
	237	7369856		2008-05-06	Ovadia, Shlomo	
	238	7428750		2008-09-23	Dunn et al.	
	239	8543814		2013-09-24	Laitinen, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	240	8700729		2014-04-15	Dua, Robin	
	241	8943551		2015-01-27	Ganapathy et al.	
	242	9413546		2016-08-09	Meier et al.	
	243	5617539		1997-04-01	Ludwig et al.	
	244	6601040		2003-07-29	Kolls, H. Brock	
	245	7486658		2009-02-03	Kumar, Rajneesh	
	246	7602746		2009-10-13	Calhoun et al.	
	247	7599714		2009-10-06	Kuzminskiy, Alexandr	
	248	7610047		2009-10-27	Hicks III et al.	
	249	7643411		2010-01-05	Andreasen et al.	
	250	8194581		2012-06-05	Schroeder et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	251	8787249		2014-07-22	Giaretta et al.	
	252	8862751		2014-10-14	Faccin et al.	
	253	7719966		2010-05-18	Luft et al.	
	254	8132256		2012-03-06	Bari, Farooq	
	255	8307095		2012-11-06	Clark et al.	
	256	8412798		2013-04-02	Wang, Frank C.	
	257	8418168		2013-04-09	Tyhurst et al.	
	258	8838686		2014-09-16	Getchius, Jeffery M.	
	259	8855620		2014-10-07	Sievers et al.	
	260	6401113		2002-06-04	Lazaridis et al.	
	261	7660419		2010-02-09	Ho, Jin-Meng	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	262	8036387		2011-10-11	Kudelski et al.	
	263	8044792		2011-10-25	Orr et al.	
	264	8140690		2012-03-20	Ly et al.	
	265	8639215		2014-01-28	McGregor et al.	
	266	8819253		2014-08-26	Simeloff et al.	
	267	7562213		2009-07-14	Timms, Natalie	
	268	8521775		2013-08-27	Poh et al.	
	269	7151764		2006-12-19	Heinonen et al.	
	270	7191248		2007-03-13	Chattopadhyay et al.	
	271	7095754		2006-08-22	Benveniste, Mathilde	
	272	7136361		2006-11-14	Benveniste, Mathilde	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	273	8402165		2013-03-19	Deu-Ngoc et al.	
	274	7409569		2008-08-05	Illowsky et al.	
	275	8125897		2012-02-28	Ray et al.	
	276	8531954		2013-09-10	McNaughton et al.	
	277	6879825		2005-04-12	Daly, Brian Kevin	
	278	6115823		2000-09-05	Velasco et al.	
	279	7203721		2007-04-10	Ben-Efraim et al.	
	280	7219123		2007-05-15	Fiechter et al.	
	281	7505795		2009-03-17	Lim et al.	
	282	9326173		2016-04-26	Luft, Achim	
	283	7389412		2008-06-17	Sharma et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	284	7466652		2008-12-16	Lau et al.	
	285	7512131		2009-03-31	Svensson et al.	
	286	7526541		2009-04-28	Roese et al.	
	287	8539544		2013-09-17	Garimella et al.	
	288	9111088		2015-08-18	Ghai et al.	

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	1567818A	CN		2005-01-19	Huawei Tech. Co. Ltd.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	2	2006012610	WO		2006-02-02	Citrix Systems, Inc.		
	3	1508734A	CN		2004-06-30	Chinese Creative Corp.		
	4	2688553	CA		2008-12-04	Yoggie Security Systems, Inc.		
	5	1850575	EP		2007-10-31	Research In Motion Limited		
	6	2003017063	WO	A2	2003-02-27	Apogee Networks		
	7	2002067616	WO	A1	2002-08-29	Sonera Oyj		
	8	2011002450	WO	A1	2011-01-06	Alcatel-Lucent USA Inc.		
	9	2003017065	WO	A2	2003-02-27	Apogee Networks		
	10	1545114	EP	A1	2005-06-22	Alcatel		
	11	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	12	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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	13	1878160	CN	A	2006-12-13	Huawei Technologies Co., Ltd.		

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.	T5
	1	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	
	2	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	
	3	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	
	4	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	
	5	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	
	6	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	
	7	Loopt User Guide, metroPCS, 7/17/2008	
	8	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	'Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	
	10	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	
	11	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	
	12	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	
	13	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	
	14	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	
	15	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	
	16	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	17	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	18	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	19	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	21	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	22	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	
	23	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	24	Roy et al., "Energy Management in Mobile Devices with the Cinder Operating System", Stanford University, MIT CSAIL, June 3, 2010	
	25	Windows7 Power Management, published April 2009	
	26	Quintana, David, "Mobile Multitasking," April 14, 2010	
	27	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	

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

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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2017-03-21
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	6	20020199001		2002-12-26	WENOCUR et al.	
	7	20030004937		2003-01-02	SALMENKAITA et al.	
	8	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	9	20030013434		2003-01-16	ROSENBERG et al.	
	10	20030018524		2003-01-23	FISHMAN et al.	
	11	20030046396		2003-03-06	RICHTER et al.	
	12	20030050070		2003-03-13	MASHINSKY et al.	
	13	20030050837		2003-03-13	KIM, Do Sik	
	14	20030088671		2003-05-08	KLINKER et al.	
	15	20030133408		2003-07-17	CHENG et al.	
	16	20030161265		2003-08-28	CAO et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	17	20030182420		2003-09-25	JONES et al.	
	18	20030182435		2003-09-25	REDLICH et al.	
	19	20030220984		2003-11-27	JONES et al.	
	20	20030224781		2003-12-04	MILFORD et al.	
	21	20030229900		2003-12-11	REISMAN, Richard	
	22	20030236745		2003-12-25	HARTSELL et al.	
	23	20040019539		2004-01-29	RAMAN et al.	
	24	20040021697		2004-02-05	BEATON et al.	
	25	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	26	20040044623		2004-03-04	WAKE et al.	
	27	20040047358		2004-03-11	CHEN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	28	20040073672		2004-04-15	FASCENDA, Anthony C.	
	29	20040082346		2004-04-29	SKYTT et al.	
	30	20040098715		2004-05-20	AGHERA et al.	
	31	20040103193		2004-05-27	PANDYA et al.	
	32	20040107360		2004-06-03	HERRMANN et al.	
	33	20040127200		2004-07-01	SHAW et al.	
	34	20040132427		2004-07-08	LEE et al.	
	35	20040168052		2004-08-26	CLISHAM et al.	
	36	20040198331		2004-10-07	COWARD et al.	
	37	20040236547		2004-11-25	RAPPAPORT et al.	
	38	20040249918		2004-12-09	SUNSHINE, Roger N.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	39	20050021995		2005-01-27	LAL et al.	
	40	20050048950		2005-03-03	MORPER, Hans-Jochen	
	41	20050055291		2005-03-10	BEVENTE et al.	
	42	20050055309		2005-03-10	WILLIAMS et al.	
	43	20050060266		2005-03-17	DEMELLO et al.	
	44	20050097516		2005-05-05	DONNELLY et al.	
	45	20050107091		2005-05-19	VANNITHAMBY et al.	
	46	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	47	20050166043		2005-07-28	ZHANG et al.	
	48	20050183143		2005-08-18	ANDERHOLM et al.	
	49	20050198377		2005-09-08	FERGUSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	50	20050216421		2005-09-29	BARRY et al.	
	51	20050228985		2005-10-13	YLIKOSKI et al.	
	52	20050238046		2005-10-27	HASSAN et al.	
	53	20050246282		2005-11-03	NASLUND et al.	
	54	20050250508		2005-11-10	GUO et al.	
	55	20050254435		2005-11-17	MOAKLEY et al.	
	56	20050266825		2005-12-01	CLAYTON, Steve	
	57	20050266880		2005-12-01	GUPTA, Vivek G.	
	58	20060014519		2006-01-19	MARSH et al.	
	59	20060019632		2006-01-26	CUNNINGHAM et al.	
	60	20060026679		2006-02-02	ZAKAS, Philip H.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	61	20060034256		2006-02-16	ADDAGATLA et al.	
	62	20060040642		2006-02-23	BORIS et al.	
	63	20060045245		2006-03-02	AARON et al.	
	64	20060048223		2006-03-02	LEE et al.	
	65	20060072646		2006-04-06	FEHER, Kamilo	
	66	20060085543		2006-04-20	HRASTAR et al.	
	67	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	68	20060143098		2006-06-29	LAZARIDIS, Mihal	
	69	20060165060		2006-07-27	DUA, Robin	
	70	20060178917		2006-08-10	MERRIAM et al.	
	71	20060178918		2006-08-10	MIKURAK, Michael G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	72	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	73	20060190314		2006-08-24	HERNANDEZ, Rick	
	74	20060199608		2006-09-07	DUNN et al.	
	75	20060206904		2006-09-14	WATKINS et al.	
	76	20060218395		2006-09-28	MAES, Stephane H.	
	77	20060233108		2006-10-19	KRISHNAN, Murali R.	
	78	20060233166		2006-10-19	BOU-DIAB et al.	
	79	20060236095		2006-10-19	SMITH et al.	
	80	20060242685		2006-10-26	HEARD et al.	
	81	20060258341		2006-11-16	MILLER et al.	
	82	20060291477		2006-12-28	CROAK et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	83	20070019670		2007-01-25	FALARDEAU, Eric	
	84	20070022289		2007-01-25	ALT et al.	
	85	20070036312		2007-02-15	CAI et al.	
	86	20070055694		2007-03-08	RUGE et al.	
	87	20070061243		2007-03-15	RAMER et al.	
	88	20070076616		2007-04-05	NGO et al.	
	89	20070093243		2007-04-26	KAPADEKAR et al.	
	90	20070100981		2007-05-03	ADAMCZYK et al.	
	91	20070101426		2007-05-03	LEE et al.	
	92	20070104126		2007-05-10	CALHOUN et al.	
	93	20070130315		2007-06-07	FRIEND et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	94	20070140113		2007-06-21	GEMELOS, Steven	
	95	20070140275		2007-06-21	BOWMAN et al.	
	96	20070198656		2007-08-23	MAZZAFERRI et al.	
	97	20070220251		2007-09-20	ROSENBERG et al.	
	98	20070226225		2007-09-27	YIU et al.	
	99	20070243862		2007-10-18	COSKUN et al.	
	100	20070248100		2007-10-25	ZUBERI et al.	
	101	20070254675		2007-11-01	ZORLU OZER et al.	
	102	20070255848		2007-11-01	SEWALL et al.	
	103	20070259673		2007-11-08	WILLARS et al.	
	104	20070263558		2007-11-15	SALOMONE, Leonardo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	105	20070274327		2007-11-29	KAARELA et al.	
	106	20070282896		2007-12-06	WYDROUG et al.	
	107	20070294395		2007-12-20	STRUB et al.	
	108	20070298764		2007-12-27	CLAYTON, Steve	
	109	20080005285		2008-01-03	ROBINSON et al.	
	110	20080005561		2008-01-03	BROWN et al.	
	111	20080010452		2008-01-10	HOLTZMAN et al.	
	112	20080039102		2008-02-14	SEWALL et al.	
	113	20080049630		2008-02-28	KOZISEK et al.	
	114	20080052387		2008-02-28	HEINZ et al.	
	115	20080059474		2008-03-06	LIM, Keng	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	116	20080059743		2008-03-06	BYCHKOV et al.	
	117	20080060066		2008-03-06	WYNN et al.	
	118	20080062900		2008-03-13	RAO, Bindu Rama	
	119	20080064367		2008-03-13	NATH et al.	
	120	20080066149		2008-03-13	LIM, Keng	
	121	20080066150		2008-03-13	LIM, Keng	
	122	20080082643		2008-04-03	STORRIE et al.	
	123	20080083013		2008-04-03	SOLIMAN et al.	
	124	20080095339		2008-04-24	ELLIOTT et al.	
	125	20080098062		2008-04-24	BALIA, Hinal K.	
	126	20080109679		2008-05-08	WRIGHT et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	127	20080120688		2008-05-22	QIU et al.	
	128	20080127304		2008-05-29	GINTER et al.	
	129	20080130534		2008-06-05	TOMIOKA, Tazuko	
	130	20080130656		2008-06-05	KIM et al.	
	131	20080132268		2008-06-05	CHOI-GROGAN et al.	
	132	20080134330		2008-06-05	KAPOOR et al.	
	133	20080147454		2008-06-19	WALKER et al.	
	134	20080160958		2008-07-03	ABICHANDANI et al.	
	135	20080162637		2008-07-03	ADAMCZYK et al.	
	136	20080162704		2008-07-03	POPLETT et al.	
	137	20080164304		2008-07-10	NARASIMHAN et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	138	20080167027		2008-07-10	GAUTIER et al.	
	139	20080167033		2008-07-10	BECKERS, Michel	
	140	20080168523		2008-07-10	ANSARI et al.	
	141	20080177998		2008-07-24	APSANGI et al.	
	142	20080183812		2008-07-31	PAUL et al.	
	143	20080184127		2008-07-31	RAFEY et al.	
	144	20080189760		2008-08-07	ROSENBERG et al.	
	145	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	146	20080212470		2008-09-04	CASTANEDA et al.	
	147	20080221951		2008-09-11	STANFORTH et al.	
	148	20080222692		2008-09-11	ANDERSSON et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	149	20080225748		2008-09-18	KHEMANI et al.	
	150	20080229385		2008-09-18	FEDER et al.	
	151	20080229388		2008-09-18	MAES, Stephane H.	
	152	20080256593		2008-10-16	VINBERG et al.	
	153	20080268813		2008-10-30	MAES, Stephane H.	
	154	20080298230		2008-12-04	LUFT et al.	
	155	20080305793		2008-12-11	GALLAGHER et al.	
	156	20080311885		2008-12-18	DAWSON et al.	
	157	20080316923		2008-12-25	FEDDERS et al.	
	158	20080318547		2008-12-25	BALLOU et al.	
	159	20080318550		2008-12-25	DeATLEY, Dallas	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	160	20080319879		2008-12-25	CARROLL et al.	
	161	20090005005		2009-01-01	FORSTALL et al.	
	162	20090013157		2009-01-08	BEAULE, Stephane	
	163	20090054030		2009-02-26	GOLDS, David	
	164	20090068984		2009-03-12	BURNETT, R. Alan	
	165	20090077622		2009-03-19	BAUM et al.	
	166	20090079699		2009-03-26	SUN, Jian	
	167	20090113514		2009-04-30	HU, Q. James	
	168	20090125619		2009-05-14	ANTANI, Snehal S.	
	169	20090180391		2009-07-16	PETERSEN et al.	
	170	20090197585		2009-08-06	AARON, Jeffrey A.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	171	20090257379		2009-10-15	ROBINSON et al.	
	172	20090271514		2009-10-29	THOMAS et al.	
	173	20090286507		2009-11-19	O'NEIL et al.	
	174	20090287921		2009-11-19	ZHU et al.	
	175	20090288140		2009-11-19	HUBER et al.	
	176	20100017506		2010-01-21	FADELL, Anthony	
	177	20100042675		2010-02-18	FUJII, Hiroshi	
	178	20100043068		2010-02-18	VARADHAN et al.	
	179	20100071053		2010-03-18	ANSARI et al.	
	180	20100082431		2010-04-01	RAMER et al.	
	181	20100103820		2010-04-29	FULLER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	182	20100188975		2010-07-29	RALEIGH, Gregory G.	
	183	20100188990		2010-07-29	RALEIGH, Gregory G.	
	184	20100188992		2010-07-29	RALEIGH, Gregory G.	
	185	20100188994		2010-07-29	RALEIGH, Gregory G.	
	186	20100191576		2010-07-29	RALEIGH, Gregory G.	
	187	20100191612		2010-07-29	RALEIGH, Gregory G.	
	188	20100191846		2010-07-29	RALEIGH, Gregory G.	
	189	20100192170		2010-07-29	RALEIGH, Gregory G.	
	190	20100192212		2010-07-29	RALEIGH, Gregory G.	
	191	20100195503		2010-08-05	RALEIGH, Gregory G.	
	192	20100197268		2010-08-05	RALEIGH, Gregory G.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	193	20100198698		2010-08-05	RALEIGH et al.	
	194	20100198939		2010-08-05	RALEIGH, Gregory G.	
	195	20100325420		2010-12-23	KANEKAR, Tushar	
	196	20110126141		2011-05-26	KING et al.	
	197	20080132201		2008-06-05	KARLBERG, Johan	
	198	20080081606		2008-04-03	COLE, Terry L.	
	199	20090248883		2009-10-01	SURYANARAYANA et al.	
	200	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	201	20080085707		2008-04-10	FADELL, Tony	
	202	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	203	20080219268		2008-09-11	DENNISON, Larry R.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20120029718		2012-02-02	DAVIS, Edward L.	
	212	20110241624		2011-10-06	PARK, Jun-seok et al.	
	213	20090307746		2009-12-10	DI, Jinwen et al.	
	214	20050009499		2005-01-13	KOSTER, Karl	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	215	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	216	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	217	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	218	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	219	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	220	20080313730		2008-12-18	Iftimie, Sorin et al.	
	221	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	222	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	223	20080240373		2008-10-02	WILHELM, Robert D.	
	224	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	225	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	226	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	227	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	228	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	229	20090172077		2009-07-02	ROXBURGH, David et al.	
	230	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	231	20030171112		2003-09-11	Lupper, Alfred et al.	
	232	20070300252		2007-12-27	Acharya, Swarup et al.	
	233	20050007993		2005-01-13	Chambers, Mahdi et al.	
	234	20020164983		2002-11-07	Raviv, Li-On et al.	
	235	20070280453		2007-12-06	Kelley, Sean S.	
	236	20100241544		2010-09-23	Benson, Dan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	237	20090157792		2009-06-18	Fiatal, Trevor	
	238	20070109983		2007-05-17	Shankar, Rohit et al.	
	239	20020049074		2002-04-25	Eisinger, Bernd et al.	
	240	20020161601		2002-10-31	Nauer, Bernhard et al.	
	241	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	242	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	243	20010048738		2001-12-06	Baniak, Paul G. et al.	
	244	20070033197		2007-02-08	Scherzer, Shimon et al.	
	245	20110013569		2011-01-20	Scherzer, Shimon et al.	
	246	20110159818		2011-06-30	Scherzer, Shimon et al.	
	247	20120020296		2012-01-26	Scherzer, Shimon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	248	20120196644		2012-08-02	Scherzer, Shimon et al.	
	249	20120238287		2012-09-20	Scherzer, Shimon	
	250	20130058274		2013-03-07	Scherzer, Shimon et al.	
	251	20130084835		2013-04-04	Scherzer, Shimon et al.	
	252	20090005000		2009-01-01	Baker, Matthew et al.	
	253	20090006116		2009-01-01	Baker, Matthew et al.	
	254	20090006200		2009-01-01	Baker, Matthew et al.	
	255	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	256	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	257	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	258	20130065555		2013-03-14	Baker, Matthew Donald et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	259	20120155296		2012-06-21	Kashanian, Nematolah	
	260	20120330792		2012-12-27	Kashanian, Nematolah	
	261	20130030960		2013-01-31	Kashanian, Nematolah	
	262	20130095787		2013-04-18	Kashanian, Nematolah	
	263	20130117140		2013-05-09	Kashanian, Nematolah	
	264	20130183937		2013-07-18	Neal, Daniel John et al.	
	265	20060135144		2006-06-22	Jothipragasam, Premkumar	
	266	20080089295		2008-04-17	Keeler, James D. et al.	
	267	20080022354		2008-01-24	Grewal, Karanvir et al.	
	268	20040102182		2004-05-27	Reith, Lothar et al.	
	269	20030233332		2003-12-18	Keeler, James D. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	270	20080250053		2008-10-09	Aaltonen, Janne et al.	
	271	20110195700		2011-08-11	Kukuchka, Robert et al.	
	272	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	273	20130144789		2013-06-06	Aaltonen, Janne et al.	
	274	20100131584		2010-05-27	Johnson, William J.	
	275	20100080202		2010-04-01	Hanson, Mark	
	276	20070147324		2007-06-28	McGary, Faith	
	277	20130024914		2013-01-24	Ahmed, Shahid et al.	
	278	20130103376		2013-04-25	Gaddam, Venkat et al.	
	279	20130111572		2013-05-02	Gaddam, Venkat et al.	
	280	20130117382		2013-05-09	Gaddam, Venkat et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	281	20130149994		2013-06-13	Gaddam, Venkat et al.	
	282	20070168499		2007-07-19	Chu, Jing-Long	
	283	20070025301		2007-02-01	Petersson, Justus et al.	
	284	20070140145		2007-06-21	Kumar, Surender et al.	
	285	20080120129		2008-05-22	Seubert, Michael et al.	
	286	20060174035		2006-08-03	Tufail, Mudassir	
	287	20110264923		2011-10-27	Kocher, Paul C. et al.	
	288	20080201266		2008-08-21	Chua, Huina et al.	
	289	20060156398		2006-07-13	Ross, Alan D. et al.	
	290	20060173959		2006-08-03	McKelvie, Samuel J. et al.	
	291	20100284327		2010-11-11	Miklos, Gyorgy	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	292	20070033194		2007-02-08	Srinivas, Davanum M. et al.	
	293	20050079863		2005-04-14	Macaluso, Anthony G.	
	294	20060114832		2006-06-01	Hamilton, Thomas E. et al.	
	295	20040225898		2004-11-11	Frost, D. Gabriel et al.	
	296	20080070550		2008-03-20	Hose, David Alan	
	297	20110019574		2011-01-27	Malomsoky, Szaboles et al.	
	298	20030188117		2003-10-02	Yoshino, Kenji et al.	
	299	20040255145		2004-12-16	Chow, Jerry	
	300	20050055595		2005-03-10	Frazer, Mark et la.	

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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	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]
	1		

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

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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2017-03-21
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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	9137389		2015-09-15	Neal et al.	
	2	8799227		2014-08-05	Ferguson et al.	
	3	9002322		2015-04-07	Cotterill, Stephen Hayden	
	4	9361451		2016-06-07	Oberheide et al.	
	5	9369959		2016-06-14	Ruutu et al.	

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	20070259656		2007-11-08	Jeong, Jong Woo	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	2	20080263348		2008-10-23	Zaltsman, Etai et al.	
	3	20080313315		2008-12-18	Karaoguz, Jeyhan et al.	
	4	20090282127		2009-11-12	LeBlanc, Michael et al.	
	5	20100167696		2010-07-01	Smith, Christopher David et al.	
	6	20030188006		2003-10-02	Bard, Steven R.	
	7	20060160536		2006-07-20	Chou, Joey	
	8	20060168128		2006-07-27	Sistla, Amber et al.	
	9	20040203833		2004-10-14	Rathunde, Dale F. et al.	
	10	20050186948		2005-08-25	Gallagher, Michael D. et al.	
	11	20070147317		2007-06-28	Smith, Brian K. et al.	
	12	20080270212		2008-10-30	Blight, Jeffrey et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	13	20080056273		2008-03-06	Pelletier, Ghyslain et al.	
	14	20110110309		2011-05-12	Bennett, James D.	
	15	20100030890		2010-02-04	Dutta, Satadip et al.	
	16	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	
	17	20080025230		2008-01-31	Patel, Alpesh et al.	
	18	20040170191		2004-09-02	Guo, Zihua et al.	
	19	20020188732		2002-12-12	Buckman, Charles R. et al.	
	20	20080034419		2008-02-07	Mullick, Amarnath et al.	
	21	20080010379		2008-01-10	Zhao, Hang	
	22	20080139210		2008-06-12	Gisby, Doug et al.	
	23	20040243992		2004-12-02	Gustafson, James P. et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	24	20070226775		2007-09-27	Andreasen, Flemming Stig et al.	
	25	20100235329		2010-09-16	Koren, David et al	
	26	20090254857		2009-10-08	Romine, Christopher et al.	
	27	20120101952		2012-04-26	Raleigh, Gregory G. et al.	
	28	20080166993		2008-07-10	Gautier et al.	
	29	20040137890		2004-07-15	Kalke, Catherine	
	30	20070143824		2007-06-21	Shahbazi, Majid	
	31	20070266422		2007-11-15	Germano et al.	
	32	20090044185		2009-02-12	Krivopaltsev, Eugene	
	33	20040039792		2004-02-26	Nakanishi, Tomoaki	
	34	20050075115		2005-04-07	Corneille et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	35	20050239447		2005-10-27	Holzman et al.	
	36	20070213054		2007-09-13	Han, Seung-Wook	
	37	20080032715		2008-02-07	Jia et al.	
	38	20090163173		2009-06-25	Williams, Timothy D.	
	39	20100075666		2010-03-25	Garner, Neil Robert	
	40	20080293395		2008-11-27	Matthews, Ajit et al.	
	41	20050245241		2005-11-03	Durand, Terry et al.	
	42	20080125079		2008-05-29	O'Neil, Douglas et al.	
	43	20050135264		2005-06-23	Popoff, Jeff et al.	
	44	20070165630		2007-07-19	Rasanen, Jorma	
	45	20100287599		2010-11-11	HE, Xianhui	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	46	20070060200		2007-03-15	Boris et al.	
	47	20060030306		2006-02-09	Kuhn, Brian Gerald	
	48	20060035631		2006-02-16	White et al.	
	49	20060206709		2006-09-14	Labrou et al.	
	50	20090046707		2009-02-19	Smires et al.	
	51	20100311402		2010-12-09	Srinivasan et al.	
	52	20110277019		2011-11-10	Pritchard Jr., John Russell	
	53	20050250536		2005-11-10	Deng et al.	
	54	20070192460		2007-08-16	Choi et al.	
	55	20080080457		2008-04-03	Cole, Terry L.	
	56	20090049518		2009-02-19	Roman et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	57	20100248719		2010-09-30	Scholaert, Hugh	
	58	20060072451		2006-04-06	Ross, Alan D.	
	59	20070294410		2007-12-20	Pandya et al.	
	60	20070293191		2007-12-20	Mir et al.	
	61	20110145920		2011-06-16	Mahaffey et al.	
	62	20130326356		2013-12-05	Zheng et al.	
	63	20070005795		2007-01-04	Gonzalez, Ruben	
	64	20080282319		2008-11-13	Fontijn et al.	
	65	20080050715		2008-02-28	Golczewski et al.	
	66	20040259534		2004-12-23	Chaudhari et al.	
	67	20090197612		2009-08-06	Kiiskinen, Arto	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	68	20100151866		2010-06-17	Karpov et al.	
	69	20060143066		2006-06-29	Calabria, Hermann	
	70	20120166604		2012-06-28	Fortier et al.	
	71	20040133668		2004-07-08	Nicholas III, Henry T.	
	72	20070073899		2007-03-29	Judge et al.	
	73	20060136882		2006-06-22	Noonan et al.	
	74	20070234402		2007-10-04	Khosravi et al.	
	75	20020154751		2002-10-24	Thompson et al.	
	76	20030084321		2003-05-01	Tarquini et al.	
	77	20070174490		2007-07-26	Choi et al.	
	78	20090048913		2009-02-19	Shenfield et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	79	20090181662		2009-07-16	Fleischman et al.	
	80	20020191573		2002-12-19	Whitehill et al.	
	81	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	82	20090070379		2009-03-12	Rappaport, Theodore R.	
	83	20100318652		2010-12-16	Samba, Augustine S.	
	84	20060095517		2006-05-04	O'Connor et al.	
	85	20040260766		2004-12-23	Barros et al.	
	86	20080034063		2008-02-07	Yee, Robert	
	87	20050041617		2005-02-24	Huotari et al.	
	88	20080018494		2008-01-24	Waite et al.	
	89	20120108225		2012-05-03	Luna et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	90	20060075506		2006-04-06	Sanda et al.	
	91	20030159030		2003-08-21	Evans, Junius A.	
	92	20070257767		2007-11-08	Beeson, Curt	
	93	20060277590		2006-12-07	Limont et al.	
	94	20090036111		2009-02-05	Danford et al.	
	95	20050096024		2005-05-05	Bicker et al.	
	96	20040127208		2004-07-01	Nair et al.	
	97	20030134650		2003-07-17	Sundar et al.	
	98	20060291419		2006-12-28	McConnell et al.	
	99	20060126562		2006-06-15	Liu, Huitao	
	100	20090203352		2009-08-13	Fordon et al.	

IPR2025-01572
Apple EX1002 Page 407

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	101	20100041365		2010-02-18	Lott et al.	
	102	20140073291		2014-03-13	Hildner et al.	
	103	20080066181		2008-03-13	Haveson et al.	
	104	20080212751		2008-09-04	Chung, Simon	
	105	20070255769		2007-11-01	Agrawal et al.	
	106	20100121744		2010-05-13	Belz et al.	
	107	20080126287		2008-05-29	Cox et al.	
	108	20030028623		2003-02-06	Hennessey et al.	
	109	20070299965		2007-12-27	Nieh et al.	
	110	20070061800		2007-03-15	Cheng et al.	
	111	20060200663		2006-09-07	Thornton, Andrew J.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	112	20050060525		2005-03-17	Schwartz et al.	
	113	20070297378		2007-12-27	Poyhonen et al.	
	114	20090006229		2009-01-01	Sweeney et al.	
	115	20090217364		2009-08-27	Salmela et al.	
	116	20050108075		2005-05-19	Douglis et al.	
	117	20070255797		2007-11-01	Dunn et al.	
	118	20090042536		2009-02-12	Bernard et al.	
	119	20090307696		2009-12-10	Vals et al.	
	120	20040176104		2004-09-09	Arcens, Suzanne	
	121	20060099970		2006-05-11	Morgan et al.	
	122	20020120370		2002-08-29	Parupudi et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	123	20040243680		2004-12-02	Mayer, Georg	
	124	20080279216		2008-11-13	Sharif-Ahmadi et al.	
	125	20040225561		2004-11-11	Hertzberg et al.	
	126	20090016310		2009-01-15	Rasal, Digambar L.	
	127	20080096559		2008-04-24	Phillips et al.	
	128	20070130283		2007-06-07	Klein et al.	
	129	20090047989		2009-02-19	Harmon et al.	
	130	20100190469		2010-07-29	Vanderveen et al.	
	131	20040267872		2004-12-30	Serdy et al.	
	132	20050091505		2005-04-28	Riley et al.	
	133	20080320497		2008-12-25	Tarkoma et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	134	20020138599		2002-09-26	Dilman et al.	
	135	20030184793		2003-10-02	Pineau, Richard A.	
	136	20040054779		2004-03-18	Takeshima et al.	
	137	20060182137		2006-08-17	Zhou et al.	
	138	20080089303		2008-04-17	Wirtanen et al.	
	139	20090132860		2009-05-21	Liu et al.	
	140	20120144025		2012-06-07	Melander et al.	
	141	20120166364		2012-06-28	Ahmad et al.	
	142	20130072177		2013-03-21	Ross et al.	
	143	20140241342		2014-08-28	Constantinof, Cristian	
	144	20070201502		2007-08-30	Abramson, Nathan	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	145	20050163320		2005-07-28	Brown et al.	
	146	20060114821		2006-06-01	Willey et al.	
	147	20080178300		2008-07-24	Brown et al.	
	148	20090049156		2009-02-19	Aronsson et al.	
	149	20080168275		2008-07-10	DeAtley et al.	
	150	20090320110		2009-12-24	Nicolson et al.	
	151	20090065571		2009-03-12	Jain, Deepak	

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	1310401A	CN		2000-02-22	Wang, Di Xing		
	2	1878160A	CN		2006-12-13	Jiang, Yong		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	3	2012047275	WO		2012-04-19	Raleigh, Gregory G. et al.		
	4	101127988A	CN		2008-02-20	ZTE Corporation		
	5	1503548 A1	EP		2005-02-02	FG Microtec GmbH		
	6	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		
	7	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		
	8	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		
	9	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		
	10	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		
	11	2009-212707	JP		2009-09-17	Fujitsu Ltd.		
	12	2008-301121	JP		2008-12-11	Kyocera Corp.		
	13	101335666A	CN		2008-12-31	Hangzhou H3C Technologies Co., Ltd.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	14	101080055A	CN		2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.			
	15	2009-232107	JP		2009-10-08	Fujitsu Ltd.			
	16	2009-111919	JP		2009-05-21	Kyocera Communications Systems			
	17	2009008817	WO		2009-01-15	Ericsson			
	18	2002045315	WO		2002-06-06	Micromuse			
	19	2009091295	WO		2009-07-23	Telefonaktiebolaget LM Ericsson			
	20	2002093877	WO		2002-11-21	Nokia Corp.			
	21	2006004784	WO		2006-01-12	Japan Communications Inc.			
	22	2005339247A	JP		2005-12-08	Secured Communications			
	23	2006155263A	JP		2006-06-15	NEC Corporation			
	24	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	25	2006-197137	JP		2006-07-27	NTT Docomo Inc.		
	26	2006-344007	JP		2006-12-21	Hitachi Ltd.		
	27	2005083934	WO		2005-09-09	Research In Motion Limited		
	28	2007120310	WO		2007-10-25	Qualcomm Inc.		
	29	2003017063	WO		2003-02-27	Apogee Networks		
	30	2002067616	WO		2002-08-29	Sonera Oyj		
	31	2011002450	WO		2011-01-06	Alcatel-Lucent USA Inc.		
	32	2003017065	WO		2003-02-27	Apogee Networks		
	33	1545114	EP		2005-06-22	Alcatel		
	34	1887732	EP		2008-02-13	Huawei Technologies Co., Ltd.		
	35	2007065	EP		2008-12-24	Huawei Technologies Co., Ltd.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	36	2006-041989	JP		2006-02-09	Fujitsu Ltd.		
	37	1289326	EP		2003-03-05	Motorola, Inc.		

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	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	
	2	3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; IP Flow Mobility and seamless WLAN offlload; Stage 2," Release 10, Document No. 3GPP TS 23.261, V1.0.0, March 2010	
	3	3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO)," Release 9, Document No. 3GPP TS 24.312, V9.1.0, March 2010	
	4	Ahmed et al., "Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS)," 2010 IEEE	

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

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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

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	/James E. Harris/	Date (YYYY-MM-DD)	2017-03-21
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 2006041989
PUBLICATION DATE : 09-02-06

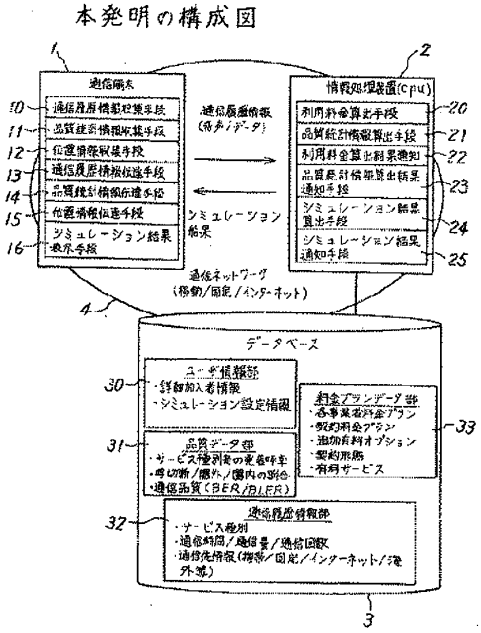
APPLICATION DATE : 28-07-04
APPLICATION NUMBER : 2004219784

APPLICANT : FUJITSU LTD;

INVENTOR : KATAOKA KOSUKE;

INT.CL. : H04M 15/16 (2006.01)

TITLE : CHARGING PLAN NOTIFICATION SYSTEM



ABSTRACT : PROBLEM TO BE SOLVED: To provide a charging plan notification system for calculating the lowest optimum charging plan corresponding to a utilization state of a communication terminal user from charging plans provided by all carriers.

SOLUTION: The charging plan notification system is provided with: a communication terminal for transmitting communication history information concerned with communication; a database 3 for storing the communication history information, all contract information between communication terminal users and communication carriers and all charging plans for communication service provided by all the carriers; and an information processor 2 for calculating utilization charges. The information processor 2 respectively calculates accurate utilization charges in the charging plans provided from respective carriers on the basis of the communication history information of each communication terminal user, the contract information and all the charging plans and notifies the communication terminal user of the calculated results.

COPYRIGHT: (C)2006,JPO&NCIPI

BNSDOCID: <JP_____2006041989A_AJ_>

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-41989
(P2006-41989A)
(43)公開日　平成18年2月9日(2006.2.9)

(51)Int.Cl.	F I	テーマコード（参考）
H04M 15/16 (2006.01)	H04M 15/16	5K025

審査請求 未請求　請求項の数 5　OL　（全 15 頁）

(21)出願番号　特願2004-219784 (P2004-219784)
(22)出願日　平成16年7月28日 (2004.7.28)

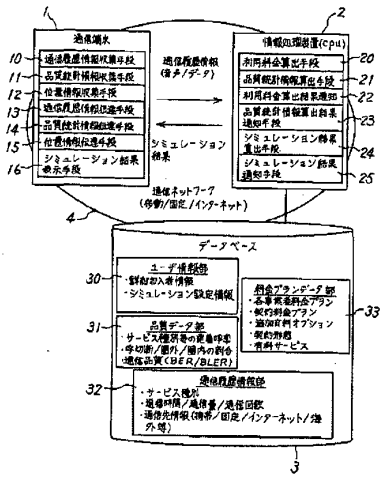
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100083297
弁理士　山谷　晧榮
(74)代理人　100087848
弁理士　小笠原　吉義
(72)発明者　友松　聖詞
東京都品川区南大井６丁目２２番７号　富士通ネットワークソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】料金プラン通知装置

(57)【要約】
【課題】全通信事業者の料金プランの中から通信端末ユーザの利用状態に応じた最も安い最適の料金プランを算出する料金プラン通知装置を提供すること。
【解決手段】このため本発明では、通信に関する通信履歴情報を送信する通信端末１と、通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベース３と、利用料金を算出する情報処理装置２を具備する料金プラン通知装置であって、通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置２により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知する。
【選択図】図１

本発明の構成図



BNSDOCID: <JP_____2006041989A__I_>

IPR2025-01572
Apple EX1002 Page 420

【特許請求の範囲】
【請求項1】
通信に関する通信履歴情報を送信する通信端末と、
通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベースと、
利用料金を算出する情報処理装置を具備する料金プラン通知装置であって、
通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知する料金プラン通知装置。
【請求項2】
前記通信端末は、全通信における発着呼率、通信途中での切断、待受け時における圏内・圏外の割合・データ伝送速度等、全ての品質情報を通信履歴情報、通信端末が取得できる位置情報とをデータベースに送信する伝達手段を持ち、
上記データベースは品質情報を蓄積する蓄積手段を持ち、
上記情報処理装置は、品質情報を基に各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出する算出手段を持ち、通信サービスの品質情報を全料金プランの正確な利用料金と共に通信端末ユーザに通知できる通知手段を具備したことを特徴とする請求項１記載の料金プラン通知装置。
【請求項3】
上記情報処理装置は、予めデータベースに登録されている、通信端末ユーザが通信事業者と契約している料金プラン、追加有料オプション、契約時期、契約形態、有料サービス、全通信事業者が提供している全料金プラン、及び有料オプション、割引情報等の情報を利用して正確な利用料金を算出することを特徴とする請求項１記載の料金プラン通知装置。
【請求項4】
上記情報処理装置は、サービス種別、通信時間、量、回数、通信先、位置情報等の詳細な通信履歴情報を利用して、正確な利用料金を算出することを特徴とする請求項１記載の料金プラン通知装置。
【請求項5】
通信端末ユーザが利用を想定した任意の利用条件をデータベースに設定し、ユーザの要求に応じて情報処理装置は、それらの情報と、データベースに登録してある通信端末ユーザの詳細加入者情報及び料金プランに関連する情報を利用して、各料金プランにおいてシミュレーションし、正確に料金算出し、結果を通信端末ユーザに通知することを特徴とする請求項１記載の料金プラン通知装置。

【発明の詳細な説明】
【技術分野】
【0001】
本発明は、通信端末の利用料金を算出し、通信端末ユーザに通知するサービスを行う料金プランを考慮した料金シミュレーションを実施し、最適な料金プランをユーザおよび事業者に通知する料金プラン通知システムに関する。
【背景技術】
【0002】
従来、携帯電話の如き通信端末では、基本使用料と一定金額の無料通話分の設定や、平日昼間や夜間、土日祝日等通話時間帯毎の通話料割引倍率、パケット料金の割引など様々な割引プランが設定されている。
【0003】
通信事業者は、これらの組み合せによりバリエーションを持たせた料金プランを準備している。
【0004】
ユーザは、あらかじめ１つの料金プランを選択し、そのプランに設定された割引率と実

IPR2025-01572
Apple EX1002 Page 421

際の月々の利用料金により算出された金額を契約した通信事業者からの請求により支払う。

【0005】

ユーザが自己の通信に対して最適な料金プランによる通信サービスを受けることができるように、ユーザに対して通話終了毎に、契約された契約料金プランと準備された全ての料金プランとを比較して、得られる最適な料金プランをリアルタイムで通知することが提案されている。

【特許文献1】特開２００１－３６６７３号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

上記従来技術では、ユーザが現在契約している通信事業者が提供しているサービスの中における最適な料金プランの提供であり、他社の通信事業者の提供しているものを含めた料金プランにおける最適なものの提供ではない。

【0007】

したがってユーザが、現在契約している料金システムが自己にとって最適なプランであるかどうかを判断するために、ユーザ自身が月々の利用状態を分析し、検討し、現在の契約通信事業者のみならず他の契約通信事業者の料金プランと比較することが必要である。

【0008】

しかるに各社の料金プランは多様・複雑化しており、ユーザ自らが分析・検討するのは困難である。したがって、各社の料金プランの中からユーザの通信端末の利用状態に応じた、最適の料金プランを提供するサービスが求められている。

【課題を解決するための手段】

【0009】

上記課題を解決するため、本発明では、下記（１）～（５）の料金プラン通知装置を提供する。

【0010】

（１）通信に関する通信履歴情報を送信する通信端末と、通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベースと、利用料金を算出する情報処理装置を具備する料金プラン通知装置であって、通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知することを特徴とする料金プラン通知装置。

【0011】

（２）上記（１）の料金プラン通知装置において、前記通信端末は、全通信における発着呼率、通信途中での切断、待受け時における圏内・圏外の割合・データ伝送速度等、全ての品質情報を通信履歴情報、通信端末が取得できる位置情報とをデータベースに送信する伝達手段を持ち、上記データベースは品質情報を蓄積する蓄積手段を持ち、上記情報処理装置は、品質情報を基に各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出する算出手段を持ち、通信サービスの品質情報を全料金プランの正確な利用料金と共に通信端末ユーザに通知できる通知手段を具備したことを特徴とする。

【0012】

（３）上記（１）の料金プラン通知装置において、上記情報処理装置は、予めデータベースに登録されている、通信端末ユーザが通信事業者と契約している料金プラン、追加有料オプション、契約時期、契約形態、有料サービス、全通信事業者が提供している全料金プラン、及び有料オプション、割引情報等の情報を利用して正確な利用料金を算出することを特徴とする。

【0013】

（４）上記（１）の料金プラン通知装置において、上記情報処理装置は、サービス種別

IPR2025-01572
Apple EX1002 Page 422

、通信時間、量、回数、通信先、位置情報等の詳細な通信履歴情報を利用して、正確な利用料金を算出することを特徴とする。

【0014】

（５）上記（１）の料金プラン通知装置において、通信端末ユーザが利用を想定した任意の利用条件をデータベースに設定し、ユーザの要求に応じて情報処理装置は、それらの情報と、データベースに登録してある通信端末ユーザの詳細加入者情報及び料金プランに関連する情報を利用して、各料金プランにおいてシミュレーションし、正確に料金算出し、結果を通信端末ユーザに通知することを特徴とする。

【発明の効果】

【0015】

本発明により下記の効果を奏する。

【0016】

（１）通信端末が通信端末ユーザの詳細な通信履歴情報をサービス提供業者の料金プラン通知装置のデータベースに登録し、情報処理装置において、前記データベースに登録された詳細な通信履歴情報と料金プラン情報を使用して、ユーザが契約していない他の通信事業者のプランも含めて全料金プランについて正確な通信料金を算出し、通信端末ユーザに通知するので、通信端末ユーザは前記契約外の通信事業者のプランも含めた一番安い料金プランを正確に知ることができる。

【0017】

（２）通信端末に、通信履歴情報と共に通話品質に関連する情報をサービス提供業者の料金プラン通知装置のデータベースに送信し、情報処理装置に、データベースに登録されている通信品質に関連する情報を使用して各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出し、通信端末ユーザに通知するので、通信端末ユーザは契約していない通信事業者のつながり易さ、音声品質等の通信品質を含め、全通信事業者の通信品質情報を知る事が出来るので、通信端末ユーザは、一番通信品質の良い通信事業者を選択することができる。

【0018】

（３）通信端末ユーザは、料金プランや契約形態等の詳細な加入者情報、契約情報をサービス提供者の料金プラン通知装置のデータベースに登録し、それらを利用料金算出に使用することにより、利用形態に沿った正確な一番安い利用料金プランを算出することが可能となる。

【0019】

（４）現在の通信端末は音声通話終話単位で表示される通信履歴情報とパケット数情報を確認できるが、これらは各通信事業者の標準的なプランを基にした情報であり必ずしも正確な情報ではなかったが、本発明では通信端末ユーザからの実用的な詳細情報の収集は、通話時間、パケット数だけでなく、通信量、通話回数、接続通話先、データ量、利用回数等通信履歴情報の詳細を用いてデータベースに登録し、それらを利用料金算出に使用できるので、情報処理装置での正確な利用料金算出を可能とする。

【0020】

（５）通信端末ユーザが自分の利用形態を想定した条件をデータベースに登録し、データベースに登録した詳細な加入者情報、各種料金プランを利用することで大雑把な料金シミュレーションではなく、正確なシミュレーションの実現が可能となり、また前月の履歴情報を流用する手段を持たせることで、シミュレーションに必要な情報を前月と同じ状態で算出することができ、ユーザオペレーションを低減させた正確なシミュレーションの実現が可能となる。

【発明を実施するための最良の形態】

【0021】

自己の通信履歴情報を、サービス業者に送信する通信端末と、多数の通信事業者の料金プランと前記通信履歴情報を保持するデータベースと、前記通信履歴情報にもとづき前記多数の通信事業者の料金プランを使用して通信を行ったときの料金を算出する情報処理装

IPR2025-01572
Apple EX1002 Page 423

置を設け、前記通信履歴情報にもとづき前記多数の通信事業者の料金プランを使用して通信を行ったときもっとも安いものを前記情報処理装置で算出して、このうちのもっとも安い料金システムを通信端末ユーザに通知する料金プラン通知装置を提供する。これにより、通信端末ユーザは、このサービス業者からの通知により、自己が契約している通信事業者以外の他の通信事業者を含めた全通信事業者の料金プランのうちより、自己に適したもっとも安い料金プランを認識することができる。

【実施例】

【0022】

本発明の実施例１を図１～図３にもとづき説明する。図１は本発明の構成図、図２は本発明の品質統計情報説明図、図３は時間毎の品質統計情報説明図である。

【0023】

図中、１は通信端末、２は情報処理装置、３はデータベース、４は通信ネットワーク、１０は通信履歴情報収集手段、１１は品質統計情報収集手段、１２は位置情報収集手段、１３は通信履歴情報伝達手段、１４は品質統計情報伝達手段、１５は位置情報伝達手段、１６はシミュレーション結果表示手段、２０は利用料金算出手段、２１は品質統計情報算出手段、２２は利用料金算出結果通知手段、２３は品質統計情報算出結果通知手段、２４はシミュレーション結果算出手段、２５はシミュレーション結果通知手段、３０はユーザ情報部、３１は品質データ部、３２は通信履歴情報部、３３は料金プランデータ部である。

【0024】

通信端末１は、ユーザが通信相手と音声やデータを送受信するものであり、例えば携帯端末である。

【0025】

情報処理装置２は、通信端末１から送信された通信履歴情報と、データベース３に保持された多くの通信事業者Ａ、Ｂ、Ｃ・・・の料金プランデータに基づいてシミュレーション演算を行い、そのうちもっとも安いものを送出するものであり、ＣＰＵで構成される。

【0026】

データベース３は通信端末１から送信された通信履歴情報や、多くの通信事業者Ａ、Ｂ、Ｃ、Ｄの料金プランデータが保持されており、外部メモリで構成されている。そしてデータベース３と情報処理装置２はサービス提供業者側の料金プラン通知装置に設置されている。

【0027】

通信ネットワーク４は、移動端末用ネットワーク、固定端末用ネットワーク、インターネットの如き、通信ネットワークである。

【0028】

通信端末１には、通信履歴情報収集手段１０、品質統計情報収集手段１１、位置情報収集手段１２、通信履歴情報伝達手段１３、品質統計情報伝達手段１４、位置情報伝達手段１５、シミュレーション結果表示手段１６等を有する。

【0029】

通信履歴情報収集手段１０は、通信端末１が通信相手に送信した送信データの種別データ量、送信時刻、送信時間、サービス種別等の履歴情報を一定期間保持するものである。

【0030】

品質統計情報収集手段１１は、通信相手から受信したデータの品質を通信相手が使用している通信事業者Ａ、Ｂ、Ｃ・・・毎に、例えば公知の５段階評価し、これを保持するものである。

【0031】

品質情報は、例えば前記受信データの５段階評価の外に、発着呼率、通信途中での切断、圏内・圏外の割合、通信品質（ビットエラーレートＢＥＲ、ブロックエラーレートＢＬＥＲ）、データ伝送レート等である。

【0032】

IPR2025-01572
Apple EX1002 Page 424

品質情報の例を図２、図３に示す。図２、図３は、通信事業者Ａ、Ｂ、Ｃ、Ｄの４者における品質統計情報を示すもので、図２（Ａ）は各通信事業者の平均の呼接続率、圏内の割合を示し、図２（Ｂ）は各通信事業者の平均の通信品質を示し、図２（Ｃ）は各通信事業者の平均データ伝送レートを示し、図３は各通信事業者の時間毎の呼接続率、圏内の割合を示す図である。

【0033】

なお図２（Ａ）における呼接続率（平均）Ｍ１と圏内の割合（平均）Ｍ２は下式により算出されるものである。

【0034】

Ｍ１＝（完了呼－不完了呼）／発呼

Ｍ２＝（圏内の時間－圏外の時間）／電源を入れていた時間

図２、図３のデータは、サービス業者に加入している通信事業者Ａ、Ｂ、Ｃ、Ｄを利用しているユーザの通信端末より送信されたデータにもとづく統計情報である。

【0035】

図２（Ａ）に示す如く、呼接続率は通信事業者Ａが約９０％、通信事業者Ｂが約９５％、通信事業者Ｃが約８０％、通信事業者Ｄが約９８％であることを示す。またノイズの少ない安定した状態で通信可能であることを示す圏内の割合は通信事業者Ａが約９５％、通信事業者Ｂが約７６％、通信事業者Ｃが約８５％、通信事業者Ｄが約９７％であることを示す。

【0036】

通信品質は、５段階評価で通信事業者Ａ、Ｂ、Ｄが５、通信事業者Ｃが４であることを示し、平均データ伝送レートは通信事業者Ａが約２５ｋｂｐｓ、通信事業者Ｂが約１７ｋｂｐｓ、通信事業者Ｃが約２３ｋｂｐｓ、通信事業者Ｄが約２４ｋｂｐｓであることを示す。

【0037】

品質情報には通信端末ユーザの住所が記入されているので、サービス装置側では各通信事業者についてこれらの住所を解析することにより例えば通信事業者Ｃが横浜駅周辺では通信品質があまりよくない等の品質統計情報を得ることができ、このような情報をユーザに提供することもできる。

【0038】

位置情報収集手段１２はサービス業者を利用している通信端末ユーザと通信先の通信端末ユーザの位置情報（住所）を収集し、これを保持するものである。

【0039】

通信履歴情報伝達手段１３は、通信履歴情報収集手段１０が収集した通信端末１が行った通信データを、通信ネットワーク４を経由してサービス業者側の情報処理装置２に送出するものである。

【0040】

品質統計情報伝達手段１４は、品質統計情報収集手段１１が収集したデータの品質情報をサービス業者側の情報処理装置２に通信ネットワーク４を経由して送出するものである。

【0041】

位置情報伝達手段１５は、位置情報収集手段１２で収集した、通信端末１と通信した相手端末のユーザの位置情報（住所）を通信ネットワーク４を経由してサービス業者側の情報処理装置２に送出するものである。

【0042】

シミュレーション結果表示手段１６は、情報処理装置２が算出したシミュレーション結果が通信ネットワーク４を経由して通信端末１に伝達されたとき、これを通信端末ユーザに表示する表示手段である。

【0043】

情報処理装置２は、通信端末から送信された通信履歴情報とデータベース４に蓄積され

IPR2025-01572
Apple EX1002 Page 425

ている全通信事業者の料金プランを使用して、全通信事業者の各料金プランについて正確な通信料金を算出し、通信端末の要求に応じて算出した通信料金を通信端末に通知したり、通信端末から受信した通信品質情報をデータベースに送信したり、データベースに登録してある通信品質情報を使用し、地域、時間帯通信事業者毎に品質統計情報を算出し通信端末の要求に応じて品質統計情報を通信端末に通知するものである。

【0044】

このため、情報処理装置２には、利用料金算出手段２０、品質統計情報算出手段２１、利用料金算出結果通知手段２２、品質統計情報算出結果通知手段２３、シミュレーション結果算出手段２４、シミュレーション結果通知手段２５等を有する。

【0045】

利用料金算出手段２０は、通信端末１から伝達された音声、データ等の通信履歴情報や、データベース部３に保持された各通信事業者の料金プランを使用して通信端末１のユーザに対する利用料金を算出するものである。

【0046】

品質統計情報算出手段２１は、通信端末１から受信されデータベース３に登録した通信品質情報を使用し、地域、時間帯、通信事業者毎における発着呼率、通信品質情報等を算出し、通信端末１の要求に応じて品質統計情報を通信端末１に通知するものである。

【0047】

利用料金算出結果通知手段２２は、利用料金算出手段２０で算出された全通信事業者の料金プランにもとづく通信料金のうち、もっとも安い料金を通信端末１に通知するものである。

【0048】

シミュレーション結果算出手段２４は、通信端末１のユーザが指定した任意の利用条件にもとづき、各通信事業者の料金プランを使用してもっとも安い利用料金を算出するものである。

【0049】

シミュレーション結果通知手段２５は、このシミュレーション結果算出手段２４から通知されたシミュレーション結果を、シミュレーション要求を行った通信端末に対し通知するものである。

【0050】

データベース３は、通信事業者に対する通信端末の加入者の詳細な契約情報、全通信事業者が提供する各種料金プラン、追加有料オプション情報、割引情報等の全ての課金に関する情報、及び本発明のサービスを制御するための、通信料金の通知回数や通知するタイミング等の設定情報、通信端末が送信した通信履歴情報を蓄積するもので、ユーザ情報部３０、品質データ部３１、通信履歴情報部３２、料金プランデータ部３３等を有し、前記情報処理装置２とともにサービス業者の料金プラン通知装置を構成する。

【0051】

ユーザ情報部３０は、通信端末１の加入者が現在契約している通信業者との詳細な契約情報である詳細加入者情報や、この加入者が料金のシミュレーション演算を求めるシミュレーション設定情報を保持するものである。

【0052】

品質データ部３１は、通信端末より送出されるサービス種別毎の発着呼率、呼切断の割合、圏内と圏外の割合、ビットエラーレート（ＢＥＲ）、ブロックエラーレート（ＢＬＥＲ）等の通信品質を保持するものである。

【0053】

通信履歴情報部３２は、通信端末より伝達された、通信端末が実際に通信を行った結果の情報を保持するもので、サービス種別、通信時間、通信量、通信回数、通信先が携帯端末か、固定端末か、インターネットか、海外か等を示す通信先情報を保持するものである。

【0054】

IPR2025-01572
Apple EX1002 Page 426

料金プランデータ部３３は、通信端末が加入しているか否かにかかわらず、全通信事業者の提供する各事業者料金プラン、契約料金プラン、追加有料オプション、契約形態、有料サービス等の課金に関する料金データを保持するものである。これらの料金データは、通信事業者がインターネットで公開したり、通信端末販売業者に郵送したりしているので、容易に入手できるものである。

【0055】

実施例１において、通信端末１は、通信履歴情報収集手段１０が収集したこの通信端末１が実際に通信した通信履歴情報を、通信履歴情報伝達手段１３が電子情報に変換し、移動通信網、固定通信網、インターネットの如き通信ネットワーク４を経由して、サービス業者の料金プラン通知装置を構成する情報処理装置２に送信する。

【0056】

情報処理装置２では、これを受信し、データベース３の通信履歴情報部３２に通信端末毎に、サービス種別、通信時間、通信量、通信回数、通信先情報等に識別して保持する。

【0057】

なお、サービス業者の料金プラン通知装置のデータベース３には、通信端末の加入者の料金プラン、オプション、契約期間等の詳細加入者情報やシミュレーション設定情報がそのユーザ情報部３０に保持され、また各通信事業者の料金プラン、契約料金プラン、追加有料オプション、契約形態、有料サービス等が料金プランデータ部３３に保持されている。

【0058】

したがって、通信端末の加入者が、例えば過去１ヶ月の通信履歴情報にもとづき、全通信事業者の料金プランにしたがって料金算出を求めたとき、情報処理装置２では、利用料金算出手段２０がデータベース３よりこの加入者の通信端末が過去１カ月に実際に通信を行った履歴情報にもとづき、料金プランデータ部３３に保持されている全通信事業者の各料金プランにより料金を算出し、これを利用料金算出結果通知手段２２に伝達する。

【0059】

利用料金算出結果通知手段２２では、この伝達された料金のうちもっとも安いものを選択してこれを通信端末１に送信する。

【0060】

通信端末１ではこれをシミュレーション結果表示手段１６が受信して表示出力し、加入者はこれにより、どの通信事業者の料金プランが自己の過去１ヶ月の通信履歴に対しもっとも安かったか認識し、現在の契約が適切か否かの判定が可能となる。勿論履歴情報は過去１ヶ月ではなく、１週間とか、適宜選択できる。

【0061】

実施例２においては、通信品質情報を算出通知するものである。通信端末１では通信毎の通信品質情報、例えば発着呼率、通信品質、通信時間、位置情報等を品質統計情報収集手段１１が算出し、これを収集する。

【0062】

品質統計情報伝達手段１４はこれらの情報を電子情報に変換し、任意のタイミングで移動通信網、固定通信網、インターネットの如き通信ネットワーク４を経由して、情報処理装置２に送信する。

【0063】

情報処理装置２は、通信端末１から受信した受信品質情報をデータベース３の品質データ部３１に送信し、通信品質情報を蓄積する。

【0064】

そして情報処理装置２は、通信端末１のユーザの要求に応じて、データベース３に登録してある通信品質情報を使用し、その品質統計情報算出手段２１が、地域毎、時間帯毎、通信事業者毎に、各時間帯毎、地域毎、事業者毎における発着呼率、呼切断、圏外・圏内の割合、ＢＥＲ、ＢＬＥＲ等の通信品質情報等を算出し、通信端末１のユーザの要求に応じて品質統計情報算出結果通知手段２３がこの品質統計情報を通信端末１に通知する。通

BNSDOCID: <JP____2006041989A__I_>

IPR2025-01572
Apple EX1002 Page 427

信端末１はこれをシミュレーション結果表示手段１６で受信してユーザに表示する。通信端末１のユーザは例えば図２、図３に示す如き、各通信事業者のサービス品質情報を取得することにより、通信サービスの品質を比較することができる。

【0065】

実施例３においては、有料オプション、契約期間等の詳細な加入者情報と、全通信事業者の提供する全料金プラン、追加オプション、割引制度情報から料金を比較算出するようにしたものである。

【0066】

データベース３のユーザ情報部３０には、情報処理装置２が通信端末ユーザの利用料金を算出する際に使用する、データベースに登録されている詳細な加入者情報が保持されている。

【0067】

この詳細な加入者情報としては、通信端末ユーザが通信事業者と契約している料金プラン情報すなわち、月額基本料金、無料通話時間、音声・データ・メール（Ｅメール、通信事業者網内向けメール、送受信料）等のサービス種別の通信料、自他国内キャリア、海外キャリア、国内・海外の固定電話、通信電話等の通信先毎の通信料、有料オプション、割引情報、契約期間、個人契約、法人契約（複数回線割引）等の契約形態等が登録されている。

【0068】

有料オプションの代表的なものとしては、通信事業者が提供する、留守番電話サービス、三者通話、海外ローミングサービス、国際通話等、その他ニュース、天気情報等の料金や条件等の詳細情報が登録される。

【0069】

割引情報の代表的なものとしては、家族割引、指定番号割引等の特定番号割引、時間帯割引、年齢・学生割引、長期契約割引、パケット割引の如きサービス種別毎の割引等の詳細情報が登録される。

【0070】

また、データベースの料金プランデータ部３３には、全通信事業者が提供している全料金プラン及び有料オプション、割引情報等の課金対象サービスの全ての詳細情報、条件が登録されており、これらの情報により情報処理装置２の利用料金算出手段２０が、例えば履歴情報に対して正確な利用料金を算出し、通信端末ユーザの契約料金と比較検討することができる。

【0071】

実施例４においては、通信履歴情報の詳細を示す。

【0072】

通信端末１がデータベース３に送信する通信履歴情報には、下記のような通信料金を算出するために必要な詳細情報が含まれている。

【0073】

音声、伝送速度・ＷＥＢアクセス・メール等のデータ、動画等のサービス種別。

【0074】

通信時間、パケット数等の量、回数。

【0075】

通信電話又は固定電話・フリーダイヤル・特定番号・ＵＲＬ・Ｅメール・国内又は海外等の通信先。

【0076】

緯経度等の位置情報。

【0077】

通信端末１は、これらの情報を電子情報に変換し、データベース３に送信する。情報処理装置２ではこれらの情報を利用料金の算出に使用する。

【0078】

IPR2025-01572
Apple EX1002 Page 428

実施例５においては、ユーザの任意の設定により、各料金プランにおいて使用料金をシミュレーション可能とするものである。

【0079】

このために、通信端末にユーザが例えば後述するサービス提供者のホームページより利用方法を想定したシミュレーション条件例えば音声通話時間、メール送受信回数、Ｗｅｂアクセス頻度、データ転送頻度、シミュレーション結果通知項目等を情報処理装置２に送信し、データベース３のユーザ情報部３０にこれらシミュレーション設定情報を登録する。

【0080】

情報処理装置２では、シミュレーション結果算出手段２４がこのシミュレーション条件と、データベース３の料金プランデータ部３３に登録ずみの全通信事業者の料金プランを利用してシミュレーション結果を算出し、シミュレーション結果通知手段２５がそのうちのもっとも安いものを通信端末１に送信し、シミュレーション結果表示手段１６がこれを表示してユーザにシミュレーション結果を知らせることができる。

【0081】

シミュレーション条件としてユーザの設定によるもののみでなく、例えばデータベースに蓄積されている前月の使用明細などの以前の通信履歴情報やデータベース３のユーザ情報部３０に予め用意してある代表的なシミュレーション条件を利用して設定することもできる。

【0082】

以前の通信履歴情報を利用する場合、本発明の料金プラン通知装置を設置するサービス提供者が作成したホームページの入力フォームにこの通信履歴情報を読み込ませるようにしてもよく、定形のファイルに以前の通信履歴情報を入力して通信端末等に送信し、通信端末は以前の通信履歴情報が記載された定形のファイルを編集し、データベースに送信することによっても実現できる。

【0083】

本発明では、通信端末ユーザは任意の利用条件を指定し、各料金プランにおいて通信料金をシミュレーションすることができる。

【0084】

通信端末は、ホームページの利用など公知の手段を使用して任意の利用条件をデータベースに設定する。任意の利用条件は、データベースに蓄積されている以前の通信履歴情報を流用することも可能である。

【0085】

データベースは通信端末から送信されてくる通信履歴情報を蓄積する。

【0086】

情報処理装置は、通信端末ユーザが指定した任意の利用条件、又はデータベースに蓄積されている以前の通信履歴情報、料金プラン、契約情報、割引情報を使用し、通信料金をシミュレーションし、通信端末ユーザに通知することができる。

【0087】

このシミュレーションとは、過去何時間とか特定の日等任意の期間の利用条件を元に、１ヶ月、１年分等の利用料金を全料金プランにおいて試算できる。これにより通信端末ユーザは種々の利用形態における利用料金を知ることができる。

【0088】

本発明では、通信端末ユーザは、情報処理装置で算出した、各料金プランの正確な使用料金、シミュレーション結果、及びサービス種別、通信先、通信時間、回数、情報量等の個別通信毎の料金内訳、品質統計情報等を下記に示す手段で入手することができる。

（１）電子データ：情報処理装置は通信端末ユーザの要求に応じて前記算出情報を、データベースから収集し、データファイル（テキスト、ＨＴＭＬ形式等）に変換して、Ｅメール、データファイルを通信端末ユーザのＥメールアドレスに送信する。また情報処理装置が前記算出情報をホームページに変換し、通信端末ユーザにホームページのアドレスを送

BNSDOCID: <JP____2006041989A__I_>

IPR2025-01572
Apple EX1002 Page 429

信し、通信端末ユーザはそのホームページのアドレスにアクセスして閲覧することにより前記情報を見ることができる。また情報処理装置が前記算出情報をデータファイルに変換して通信端末ユーザに送信し、通信端末ユーザはそのデータファイルを閲覧することにより前記算出情報を見ることができる。

【0089】

（２）前記以外の手段：情報処理装置は通信端末ユーザの要求に応じて、前記算出情報をデータベースから収集し、音声ガイダンスに変換することで通信端末ユーザに聞かせることができる。またその他に、明細書を作成して郵送したり、オペレータによる対応等により通信端末ユーザは前記算出情報を入手することができる。

【0090】

本発明では、通信端末ユーザは、情報処理装置が行う全ての処理、情報を伝送するタイミングを任意に設定することができる。これにより、通信料が安い時間帯での送信や、日、週、月、年単位等のある期間の通信履歴情報を送信するタイミング、自動又は手動、月に何回等の回数を設定することができる。これにより通信端末は、任意のタイミングで通信履歴情報をデータベースに送信することができる。

【0091】

また通信端末は、利用料金をシミュレーションさせるタイミング、シミュレーション結果を通知するタイミング等の各種タイミングをデータベースに登録することができる。

【0092】

情報処理装置は、前記タイミングで利用料金算出、シミュレーションを行い、通信端末ユーザに利用料金や、シミュレーション結果を通知する。

【0093】

本発明では、通信履歴情報や品質情報及び情報処理装置が送信するデータに優先度をつけることができ、これによりトラフィックを制御することができる。

【0094】

通信端末や情報処理装置では、公知の手段によりそれぞれが送信すべきデータの形式を変換して送信することができる。通信事業者は一般的に許容される伝送遅延を、映像＞音声＞パケットデータ（ＷＥＢアクセス、ファイル転送、Ｅメール等）の順に設定していることが多いので、通信履歴情報や品質情報、使用料金シミュレーション等の通信端末と情報処理装置で送受信する全ての情報を映像のフォーマットに変換して送れば、遅延時間は最小で送信できるが、その分トラフィックを圧迫することになる。反対にパケットデータに変換して送れば、遅延時間は多くなるが、その分トラフィックの隙間を利用して送信できるので、通信ネットワークのトラフィックに負担をあまりかけないようにできる。

【0095】

本発明では、使用料金算出、シミュレーションや品質情報を提供するのに通信費がかかるので、通信端末ユーザは、使用料金算出やシミュレーションに関連する情報を使用料金算出、シミュレーションする際に料金に含むか、含まないかをデータベースに設定することができる。もし「含まない」を選択した場合、情報処理装置は、純粋な通信にかかった使用料金を算出し、通信端末ユーザに送信する。このように通信端末ユーザは、純粋に通信にかかった料金のみを知ることができる。

【0096】

本発明では、通信端末ユーザは、情報処理装置で算出する通信先、通信時間、回数、情報量等の詳細な通信履歴毎の料金、事業者内・事業者間、比較プラン数、通知プラン数等のシミュレーション結果、料金プラン、通信履歴情報、割引情報等のシミュレーション条件の内容を、ユーザが任意に設定できる。

【0097】

これにより使用料金算出、シミュレーションにかかる通信費や情報処理装置がシミュレーションに要する時間を調整できる。

【0098】

通信端末ユーザは、使用料金算出、シミュレーション結果、シミュレーション条件の項

IPR2025-01572
Apple EX1002 Page 430

目のうち、任意の項目をデータベースに設定できる。これにより通信端末ユーザはどこまで正確に使用料金を算出するか設定することができる。当然、条件が多ければ通信履歴情報やシミュレーション結果等のデータ量は多くなり、その分通信費、情報処理装置が処理に要する時間は多くなる。

【0099】

情報処理装置は通信端末ユーザがデータベースに設定された条件を使用して使用料金算出、シミュレーションを行い通信端末ユーザに結果を送信する。

【0100】

本発明では、個人情報の秘密を保護するため、通信端末ユーザが送信する通信履歴情報及び情報処理装置において算出する使用料金算出、シミュレーション結果、品質情報等全てを暗号化して送信することができる。例えば通知端末では公知の暗号化機能を有するソフトを使用することができ、また情報処理装置は自身で暗号化機能を持つ。

【0101】

暗号化・復号化手段には一般に使用されている公開鍵暗号方式、秘密暗号方式等の暗号化手段や、ＩＤ、パスワード、電子署名等の認証機能手段が考えられる。

【0102】

暗号化手段を使用する場合は、通信端末のアプリケーションソフトと情報処理装置で同じ暗号化・復号化手段を持つ。また認証機能を使用する場合は、通信端末ユーザはデータベースにＩＤ、パスワード、電子署名等を登録しておき、情報処理装置はそれらの認証情報が一致していることが確認できたら通信端末ユーザからの情報を受信する。

【0103】

また通信端末ユーザは、情報処理装置から送信される認証情報と、予め情報処理装置から入手しておいた認証情報が一致していることが確認できたら、情報処理装置からの情報を受信する。

【0104】

本発明では、通信端末ユーザが設定する任意の使用料金設定を超えた、又は下回っている時に、通信端末ユーザにその旨を通知する機能を持つ。

【0105】

通信端末ユーザは、任意の使用料金と、その設定した使用料金を超えた、又は下回っている時に通知するようデータベースに設定する。情報処理装置はそれらの設定を認識し、通信端末ユーザから送信されてくる通信履歴情報から使用料金を算出し、データベースに設定されている使用料金を超えた、又は下回っている時に、通信端末ユーザに設定金額をいくら上回った、または下回っているかを通知する。

【0106】

本発明では、通信端末ユーザが契約している料金プランにおいて、無料通信料金が設定されている場合、通信端末ユーザに無料通信料金の残高、残り時間、残りパケットを通知する機能を持つ。

【0107】

通信端末ユーザは、データベースに無料通信料金の残高、残り時間、残りパケット数を通知させる時間、ベアラ毎の残高、残り時間、残りパケット数の割合等の内容を設定する。

【0108】

情報処理装置はそれらの設定を認識し、通信端末ユーザから送信されてくる通信履歴情報から使用料金を算出し、通信端末ユーザに、残高、残り時間、残りパケット数を通知する。

【0109】

通信端末ユーザは本発明が提供する、使用料金算出、シミュレーション、品質情報のうち、任意のサービスを選択することができる。

【0110】

通信端末ユーザは、シミュレーション内容、無料通信料金の算出、比較プラン数等デー

IPR2025-01572
Apple EX1002 Page 431

タベースに希望するサービスの種類、シミュレーション回数、品質情報等を受け取る回数、タイミングを設定する。

【0111】

情報処理装置はそれらの設定を認識し、通信端末ユーザから送信してくる通信履歴情報から使用料金、品質情報を算出し、通信端末ユーザの設定した日時に通信端末ユーザが要求した情報を送信する。

【0112】

本発明では、通信端末ユーザの加入者情報は公知のアプリケーションソフトやサービス提供者が作成するホームページを利用することでデータベースに登録、修正することができる。

【0113】

通信端末ユーザは、アプリケーションソフトを使用する場合は、アプリケーションソフトが提供するフォーマットに設定項目を入力し、データベースに送信する。ホームページを使用する場合は、通信端末ユーザが本サービス提供者が提供する加入者情報のホームページにアクセスし、必要事項を記入することで、データベースに通信端末ユーザの加入者情報を登録することができる。修正も同様の手段で可能である。

【0114】

本発明を使用すれば、通信端末ユーザは料金とサービス品質の両面から最適な料金プラン、通信事業者を選択することができる。また通信事業者は各ユーザの使用状況を詳細に把握することができ、適切な料金プランを検討する際に有効なデータや、サービスエリア拡充時に参考になる情報を得ることができる。

【図面の簡単な説明】

【0115】

【図1】本発明の一実施例構成図である。

【図2】本発明の品質統計情報説明図である。

【図3】本発明の時間毎の品質統計情報説明図である。

【符号の説明】

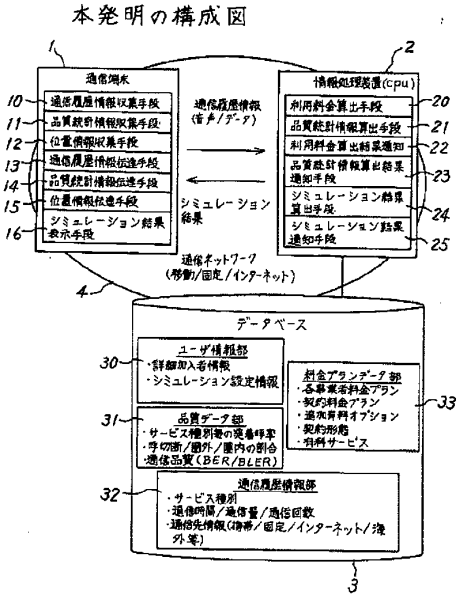
【0116】

1　通信端末
2　情報処理装置
3　データベース
4　通信ネットワーク

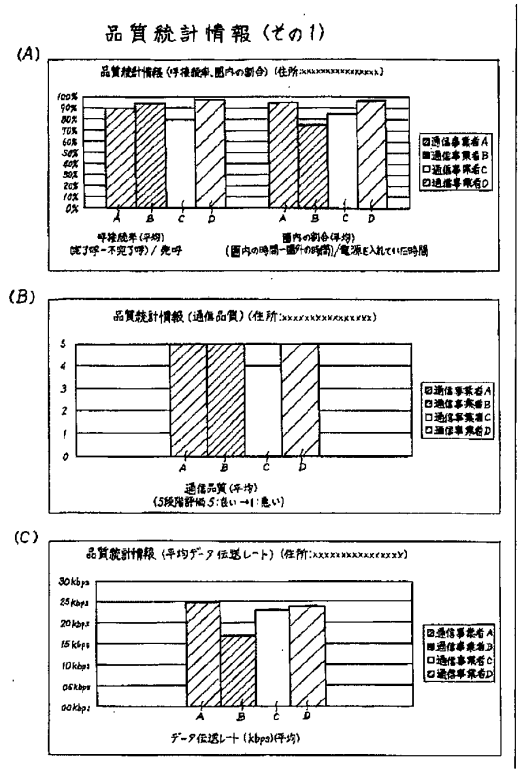
BNSDOCID: <JP_____2006041989A__|_>

IPR2025-01572
Apple EX1002 Page 432

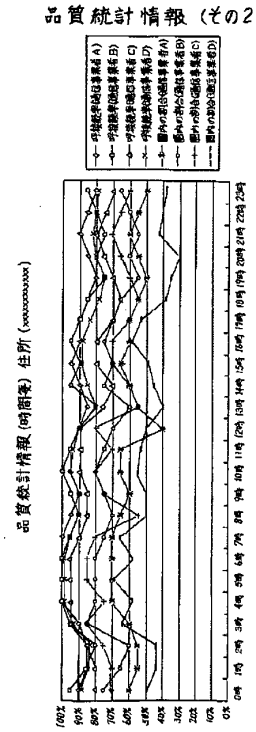
【図1】



【図2】



【図3】



BNSDOCID: <JP_____2006041989A__I_>

IPR2025-01572
Apple EX1002 Page 433

(72)発明者　片岡　康祐
東京都品川区南大井６丁目２２番７号　富士通ネットワークソリューションズ株式会社内

Ｆターム(参考) 5K025 AA08 BB06 CC01 JJ02 JJ16 JJ18

BNSDOCID: <JP_____2006041989A__I_>

IPR2025-01572
Apple EX1002 Page 434

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 289 326 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.03.2003 Bulletin 2003/10

(51) Int Cl.[7]: **H04Q 7/32**

(21) Application number: **01402259.4**

(22) Date of filing: **30.08.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **MOTOROLA, INC.**
Schaumburg, IL 60196 (US)

(72) Inventors:
- **Deloume, Pascal**
31170 Tournefeuille (FR)
- **Garani, Pradeep**
31000 Toulouse (FR)

(74) Representative: **Litchfield, Laura Marie et al**
Motorola European Intellectual Property Operations,
Midpoint - Alencon Link
Basingstoke, Hampshire RG21 7PL (GB)

(54) Method of verifying downloaded software and corresponding device

(57) The present invention relates to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software. Thus the security of the keys and calculations involving the secure keys are kept secure. Preferably root security keys stored in the smart card can be updated using communication system messaging protocols.

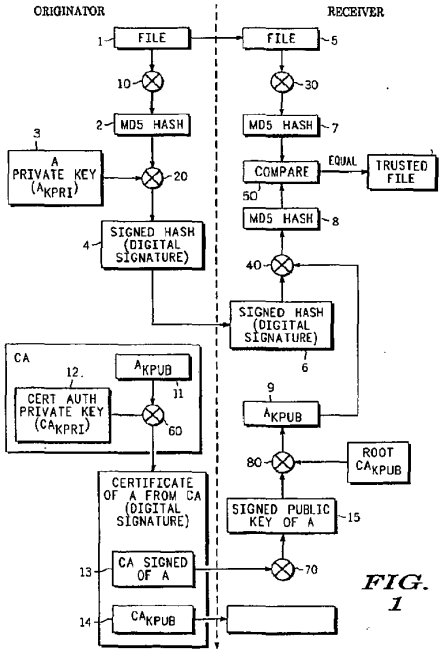


FIG. 1

EP 1 289 326 A1

Printed by Jouve, 75001 PARIS (FR)

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 435

Description

[0001] The present invention relates to a method of verifying software downloaded from an originator to a device, and to a corresponding device. In particular, the invention relates to download verification in standardised execution environments such as the Mobile Execution Environment (MExE) and Java.

[0002] Increasingly it is becoming desirable for software to be downloaded to a portable device over the air. This allows the device to be upgraded with newly released software or enables new applications to be added to the device as these become available.

[0003] It is desirable that the device checks the authenticity of the downloaded software to determine whether, for example, the downloaded software has indeed been received from a trusted sender. In addition, it is desirable that the downloaded software should be restricted to a given domain, to avoid permission violation for the rest of the device.

[0004] This security can be ensured by keys, which are stored securely in the device such that they cannot be read or tampered with by applications except the security-checking environment. In addition it is desirable to update the keys periodically, and this must be done using a secure method.

[0005] Previously, it has been suggested to implement the security algorithms in software/hardware and then to protect them by hardware control on the processor of the terminal with memory management unit. However, this results in increased cost. In addition, the development of separate security hardware is undesirable.

[0006] The Mobile Execution Environment (MExE), which enables software download, is currently under standardisation. Three class marks are defined in the MexE environment. Class mark 1 relates to devices utilizing the Wireless Application Protocol (WAP); class mark 2 relates to devices, such as personal digital assistants (pda) or laptops using standard edition JAVA™ (J2SE); and class mark 3 relates to small devices, such as mobile telephones, using micro-edition JAVA™ (J2ME).

[0007] J2ME is being proposed as an environment for class mark 3 devices in MExE because of its small size, which makes it suitable for environments, such as the mobile communication environment for example, in which the available memory or processing power is limited and the size of files must be limited.

[0008] However, the security model for J2ME requires server-based pre-verification, in which a server inserts basic run-time security information in the software prior to download. The receiving device can then use the run-time security information to check the security of the download and verify the sender.

[0009] It is desirable to increase the security provided for software download, particularly in a MExE class mark 3 environment, so that server-based verification is avoided and software can be downloaded from a greater variety of sources.

[0010] According to a first aspect of the present invention, there is provided a method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising: receiving software and security information relating to the received software; obtaining in the smart card a first calculation result from the security information using at least one secure key; obtaining in the device a second calculation result from calculations performed on the received software; and comparing in the device first and second calculation results to verify the received software.

[0011] According to a second aspect of the invention, there is provided a device comprising: communication means for receiving software and security information relating to the received software; smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key; means for obtaining a second calculation result from calculations performed on the received software; means for comparing first and second calculation results to verify the received software.

[0012] For a better understanding of the present invention, and to show how it may be brought into effect reference will now be made, by way of example to the accompanying drawings in which:

Figure 1 illustrates a known file transfer verification procedure;
Figure 2 shows a communication device;
Figure 3 illustrates a download verification procedure in accordance with the invention;
Figure 4 illustrates message creation for transfer of the root key in accordance with the invention;
Figure 5 illustrates update of the root key in accordance with the invention

[0013] The present invention is described with reference to the use of RSA cryptography. The RSA cryptography algorithm and principle are well known and therefore will not be explained in detail in this document. As will be apparent to a skilled person, other cryptography techniques may also be used in accordance with the invention.

[0014] Figure 1 illustrates a known file transfer verification procedure, for verifying the authenticity of a file transferred from an originator to a receiver. The principle behind this procedure is that in addition to the transfer of the file 1 a second piece of information which is related to both the file 1 and the originator is also transferred between the originator and the receiver, which information enables the receiver to confirm that the file comes from the originator. In addition, the receiver possesses or is passed a third piece of information, which enables

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 436

the receiver to confirm that the originator can be trusted and that it is therefore safe to execute the downloaded file.

[0015] In the illustrated procedure the originator generates the second piece of information by performing an MD5 hash operation 10 on the file 1 to be transferred to create an MD5 hash result 2. The MD5 hash operation is well known and will not be explained further. The MD5 hash result 2 is uniquely dependent on the file 1 and can be used to verify file 1.

[0016] Next the originator performs an RSA algorithm operation 20 on the MD5 hash result 2 using the private key of the originator (A_{KPRI}) 3 to generate a signed hash (or digital signature) 4. The signed hash 4 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 1 and the signed hash 4 are transferred to the receiver resulting in a received file 5 and a received signed hash 6.

[0017] In order to verify the received file, the receiver independently generates two versions of the MD5 hash result. The first MD5 hash result 7 is generated from the received file 5 using a MD5 hash operation 30, and the second MD5 hash result 8 is obtained from the received signed hash 6 by performing an RSA operation 40 on the received signed hash 6 using the public key of the originator A (A_{Kpub}) 9 held by the receiver. The first MD5 hash result 7 and the second MD5 hash result 8 are compared in a comparison operation 50 and if they are found to be equal, the received file 5 is authenticated and can be executed.

[0018] In order for the above authentication scheme to work, the receiver must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure through the use of a certification authority. The certification authority is trusted by the receiver, such that received information signed by the certification authority is trusted by the receiver.

[0019] Therefore, as shown the certification authority performs an RSA algorithm operation 60 on the public key of the originator (A_{KPub}) 11 using the private key of the certification authority (CA_{KPRI}) 12 resulting in a signed key 13 of the originator A. The signed key 13 and the certification authority public key (CA_{Kpub}) 14 are transferred to the receiver. As shown, if necessary the signed key 13 undergoes a certificate chain analysis operation 70 to obtain the received signed public key 15 of the originator A.

[0020] A certificate chain analysis operation is required if the certificate authority CA is not known by the receiver. In this case, the certificate authority is requested to provide its public key signed by a further certificate authority using the private key of the further certificate authority. If the further certificate authority is trusted by the receiver, the receiver will be able to use the public key of the further signature authority to verify that the public key of the signed authority has been signed by the private key of the further signature authority. The receiver can then trust the certificate authority and can use the received certificate authority public key. If the further certificate authority is not trusted by the receiver, use must be made of an additional certificate authority.

[0021] The receiver has stored therein a root certification authority public key. The root certification authority is the most trusted by the receiver, and ultimately the stored public key of the root certification authority can be used to verify all other certification authorities in a certificate chain situation.

[0022] The receiver then performs an RSA operation 80 on the resulting signed public key of the originator (A_{KPub}) (15) using the root certification authority public key (Root CA_{KPub}) to obtain the public key of the originator (A_{KPub}) 9. The public key of the originator (A_{KPub}) 9 is then used in the RSA operation 40 as described above.

[0023] The present invention is described below with reference to a communication device, such as a mobile telephone. However, it will be clear to a skilled person that the present invention is also applicable to other devices. An exemplary communication device 200 is now described with reference to Figure 2.

[0024] The communication device 200 shown in Figure 2 comprises a communication interface 210 coupled to an antenna 220 and to a processor 230. The processor 230 and the communication interface 210 are also coupled to volatile memory 240 and to a non-volatile memory 250. A smart card 260 is coupled to a smart card interface 270, which is also coupled to the processor 230. The smart card is equipped with its own processor 280 and memory 290.

[0025] The communication interface 210 comprises the necessary components to convert radio frequency signals for the communication device 200 received by the antenna 220 to digital signals to be stored in volatile memory 240 and/or non-volatile memory 250 and/or to be processed by processor 230, and to convert digital signals from the memories 240 and 250 and/or the processor 230 to radio frequency signals to be transmitted by the antenna 220. Thus communication interface 210 comprises radio frequency transmitter and receiver means and signal processor means, for example.

[0026] The volatile memory 240 and non-volatile memory 250 are used for storing program and other data for operation of the communication device 200.

[0027] The smart card is preferably a subscriber smart card (SIM) holding subscriber information used by the communication device 200, for example a Subscriber Identity Module card as currently used in the Global System for Mobile Communications (GSM system) and in use or proposed for other communication systems. However, it is possible that the smart card 260 may be another type of smart card received in the communication device instead of, or preferably in addition to a SIM card, for example an electronic commerce smart card.

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 437

[0028] As indicated above, the smart card is equipped with its own processor 280 and memory 290, and is capable of storing information therein and is also capable of carrying out operations or calculations on data received from the processor 230 via smart card interface 270 and of providing data or the results of such calculation to the processor 230 via smart card interface 270.

[0029] The smart card is preferably removably receivable in the communication device, for example by means of the provision of a slot in the housing of the communication device 200.

[0030] It will be appreciated by a skilled person that other components or arrangements of components within the communication device 200 are possible within the scope of the invention.

[0031] The secure download procedure in accordance with the invention will now be described with reference to Figure 3. In Figure 3 operations or data corresponding to operations or data in Figure 1 have been given similar reference numerals.

[0032] Figure 3 illustrates the download of an executable J2ME file in a MExE environment from an originator A to a device such as the communication device 200 described above with reference to Figure 2. As shown in Figure 3, box 3260 represents operations carried out and data stored in the smart card 260 of the communication device 200 shown in Figure 2, and the remaining operation and data storage is carried out in the rest of the communication device 200 shown in Figure 2.

[0033] As illustrated in Figure 2, the smart card 260 has no direct communications capability. Instead, the relevant data received by the communication device is passed by the processor 230 to the smart card 260 for storage therein and operation thereon.

[0034] In the procedure illustrated in Figure 3, the originator A performs an MD5 hash operation 310 on a file 31 to be transferred to create an MD5 hash result 32. As explained above, the MD5 hash result 32 is uniquely dependent on the file 31 and can be used to verify file 31.

[0035] Next the originator A performs an RSA algorithm operation 320 on the MD5 hash result 32 using the private key of the originator (A_{KPRI}) 33 to generate a signed hash 34. The signed hash 34 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 31 and the signed hash 34 are then sent to the communication device 200 resulting in a received file 35 and a received signed hash 36. File 35 is received using antenna 220 and communication interface 210 and is stored by the processor 230 in the volatile memory 240. In contrast, the signed hash 34 is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290.

[0036] As described above, in order to verify the received file, two versions of the MD5 hash result must be independently generated and compared. The first MD5 hash result 37 is generated by the communication device processor 230 from the received file 35 using a MD5 hash operation 330.

[0037] The second MD5 hash result 38 is obtained by the smart card from the received signed hash 36. The smart card processor 280 performs an RSA operation 340 on the received signed hash 36 stored in the smart card memory 390 using the public key of the originator A (A_{Kpub}) 39 stored in the smart card memory 290, as will be explained later.

[0038] The second MD5 hash result 38 is passed by the smart card processor 280 to the communication device processor 230 and the communication device processor 230 compares the first MD5 hash result 37 and the second MD5 hash result 38, calculated in the smart card 260, in a comparison operation 350. If the first MD5 hash result 37 and the second MD5 hash result 38 are found to be equal, the received file 35 is authenticated and can be executed.

[0039] In this arrangement, the smart card 260 must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure according to Figure 3 through the use of the root certification authority public key stored in the smart card memory 290. The root certification authority is trusted by the communications device, such that received information signed by the certification authority is trusted.

[0040] In this context, there may be more than one root certification authority. For example in the context of a mobile telephone the manufacturer and/or the operator can act as a root authority. In addition, it is possible to specify one or more trusted third parties as root certification authorities. The public key for each of the root certification authorities (eg the operator public root key (OPRK); the manufacturer public root key (MPRK); and third party public root key (TPRK)) is stored in the smart card of the communication device 200, for example during provisioning of a mobile telephone SIM card.

[0041] In order that the smart card 260 has authenticated access to the public key of the originator A (A_{Kpub}), as shown the root certification authority performs an RSA algorithm operation 360 on the public key of the originator (A_{KPub}) 311 using the private key of the certification authority ($RootCA_{KPRI}$) 312 resulting in a certificate from A 321 signed by the root certification authority. This certificate 321 is sent to the communications device 200, is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290 as certificate 322.

[0042] The Root certification authority public key ($RootCA_{KPub}$) 332 is already stored in the smart card memory 290, as indicated above. The smart card processor can perform an RSA operation 380 on the received certificate 322 using the Root Certification Authority public key ($RootCA_{KPub}$) 332 to obtain the public

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 438

key of the originator A (A_{Kpub}) 39. The smart card processor can then use the obtained public key of the originator A (A_{Kpub}) 39 and the received signed hash 36 in RSA operation 340 to obtain the smart card MD5 hash value 38, as outlined above.

[0043] Also shown in Figure 3 is the transfer of the Root Certification Authority public key ($RootCA_{KPub}$) 331 to the communications device for storage in the smart card memory as Root Certification Authority public key ($RootCA_{KPub}$) 332. It is desirable to update the root certification authority keys periodically in a secure manner otherwise the security of the system will be compromised.

[0044] A preferred mechanism for the secure transfer of a Root public key (for example OPRK, MPRK, TPRK) using communication system messaging technology will now be explained with reference to Figures 4 and 5.

[0045] Figure 4 illustrates message creation for transfer of a root key, for example the operator public root key (OPRK), to the smart card 360 in accordance with the invention. In this exemplary arrangement, the update is achieved using a SMS message as provided in the GSM/UMTS systems, although other messaging techniques could be used.

[0046] An RSA operation is performed on the new OPRK 41 with the operator's private root key 42 corresponding to the old OPRK stored in the smart card 360. As mentioned earlier, the old OPRK may have been stored in the smart card 360 during provisioning, or during a previous update of the root key. The resulting signed new operator public root key 44 is included in an SMS message 45 to be sent to the communication device. The SMS message 45 has an SMS header portion 451 and SMS download command 452 in addition to the signed new operator public root key 44. The SMS message in encrypted by the communication system prior to being sent to the communication device.

[0047] Figure 5 illustrates update of the root key in the communication device in accordance with an embodiment of the invention. In this exemplary embodiment of the invention, the SMS message 45 sent by the network 500 to the communication device 200 is passed to the smart card 260. Once the encrypted SMS message 45 is received in the smart card 260, the smart card 260 undertakes an SMS message analysis and memory update procedure 51.

[0048] In the SMS message analysis and memory update procedure 51 the SMS message is initially decrypted and the SMS message is analysed. The download command 452 instructs the smart card 260 that a new OPRK is being sent to the smart card 260. The smart card 260 performs an RSA operation on the received signed new OPRK using the old OPRK already stored in the smart card 260 to verify the identity of the sender. The OPRK stored in the smart card can then be updated using the new value. Preferably a confirmation message 52 is sent from the smart card 260 to the network using the communication interface 210 of the communication device 200.

[0049] Although the update of the operator public root key (OPRK) has been described above, it would be possible to update any root key stored in the smart card in the same way.

[0050] In accordance with an alternative embodiment of the invention, the manufacturer root public key may be stored partially in the smart card memory and partially in the communications device memory. This arrangement is more secure since the communication device then contributes to ensuring the security of download in the manufacturer domain using the manufacturer root public key. This helps to prevent an insecure smart card from changing the manufacturer public root key via download authorization.

[0051] Thus the present invention proposes a solution to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software.

[0052] Since the secure keys are stored on the smart card and calculations involving the secure keys are performed by the smart card, the security of the secure keys can be ensured. In addition, the result of the calculation performed on the received file by the device is not passed to the smart card.

[0053] As will be apparent to a skilled person, the invention could be implemented in a different form from that shown herein, and so the invention is intended to encompass all arrangements and variations within the scope of the appended claims.

Claims

1. A method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising:

   receiving software and security information relating to the received software;
   obtaining in the smart card a first calculation result from the security information using at least one secure key;
   obtaining in the device a second calculation result from calculations performed on the received software; and
   comparing in the device first and second calculation results to verify the received software.

2. The method as claimed in claim 1, further comprising the steps of;

   receiving additional signed originator key infor-

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 439

mation;
obtaining, in the smart card, originator key information from the received signed originator key information using a root security key stored therein; and
obtaining in the smart card the first calculation result from the security information using the originator key information.

3. The method as claimed in claim 2 wherein the root security key stored in the smart card is updated by
receiving a root security key update message containing a new root security key;
verifying the new root security key using the existing root security key stored in the smart card;
storing the new root security key in the smart card.

4. The method as claimed in claim 2 or 3, wherein part of the root security key is stored in the smart card and part of the root security key is stored in the device.

5. The method as claimed in any preceding claim, wherein the smart card is a Subscriber Identity Module (SIM) card

6. A device comprising
communication means for receiving software and security information relating to the received software;
smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key;
means for obtaining a second calculation result from calculations performed on the received software;
means for comparing first and second calculation results to verify the received software.

7. The device as claimed in claim 6 wherein
the communications means also receives additional signed originator key information; and
the smart card interface also passes the additional signed originator key information to the smart card, which obtains originator key information from the received signed originator key information using a root security key stored therein; and obtains the first calculation result from the security information using the originator key information.

8. The device as claimed in claim 7 wherein
the communications means also receives a root security key update message containing a new root security key; and
the smart card interface passes the root security key update message to the smart card, which verifies the new root security key using the existing root security key stored in the smart card; and stores the new root security key in the smart card.

9. The device as claimed in claim 7 or 8, wherein the device comprises storage means and part of the root security key is stored in the smart card and part of the root security key is stored in the storage means.

10. The device as claimed in one of claims 6-9, wherein the smart card is a Subscriber Identity Module (SIM) card.

BNSDOCID: <EP_____1269326A1_I_>

IPR2025-01572
Apple EX1002 Page 440

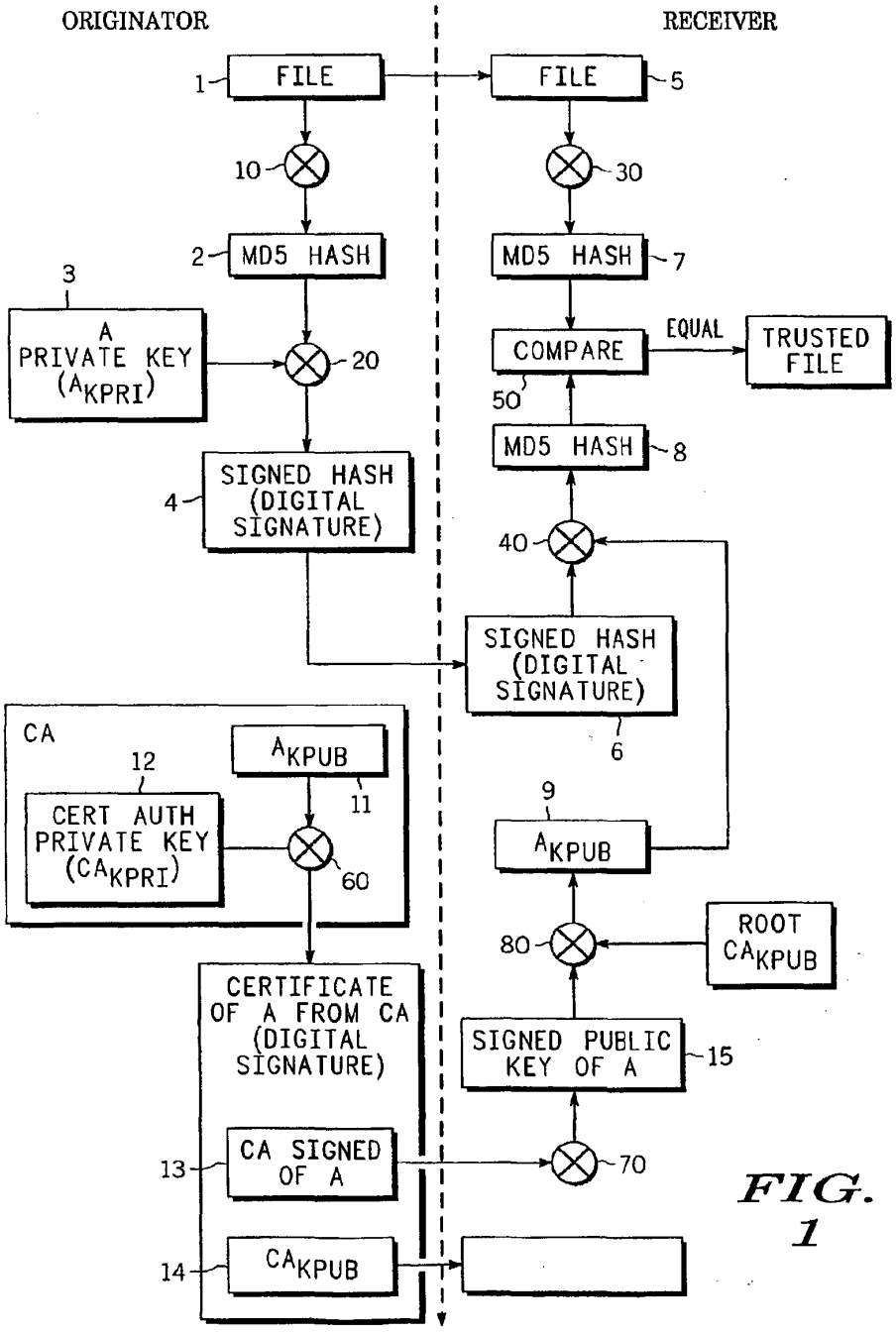


FIG. 1

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 441

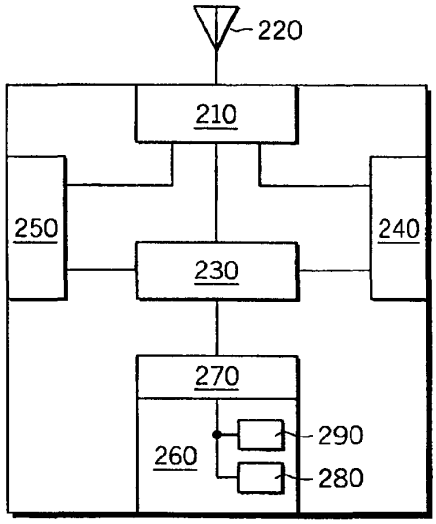


FIG. 2

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 442

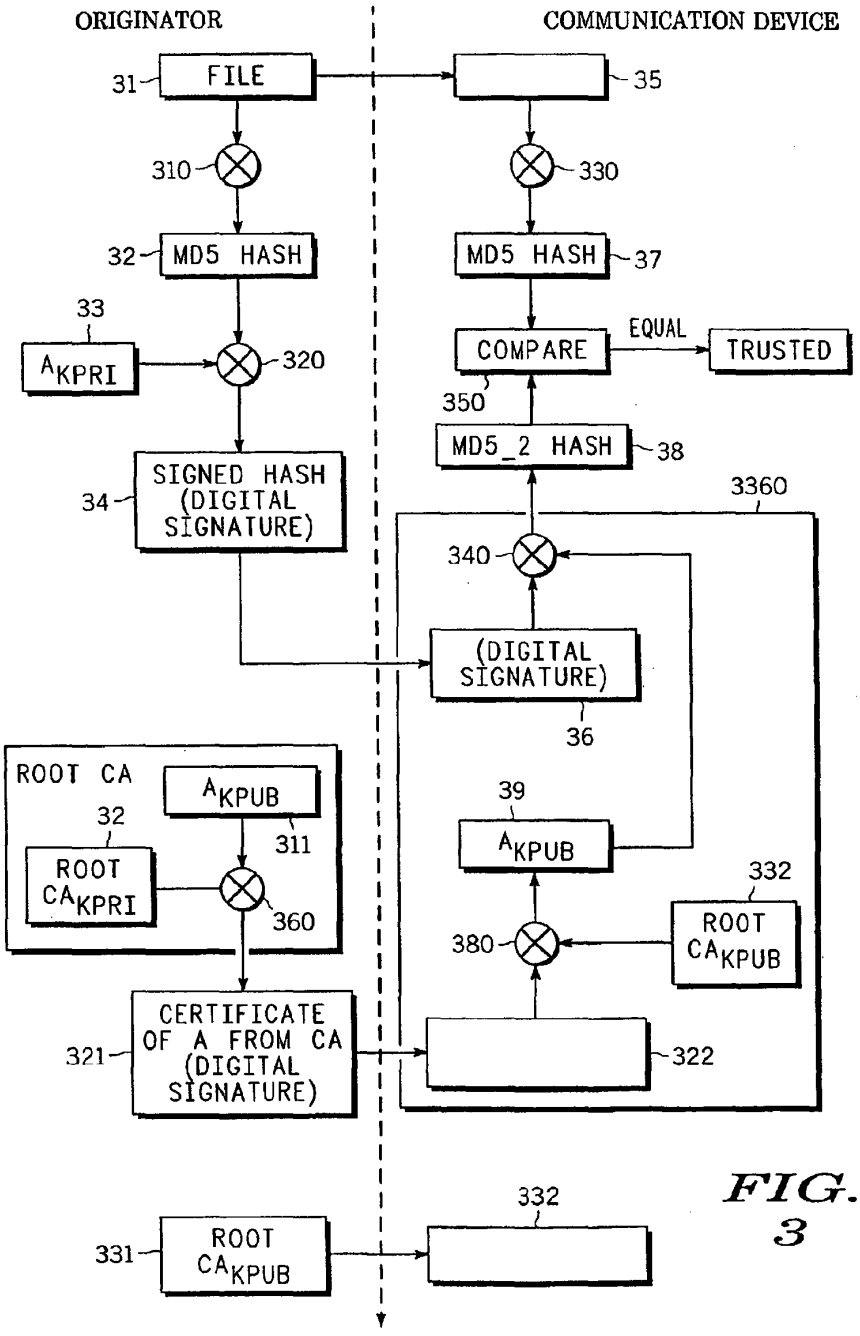


FIG. 3

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 443

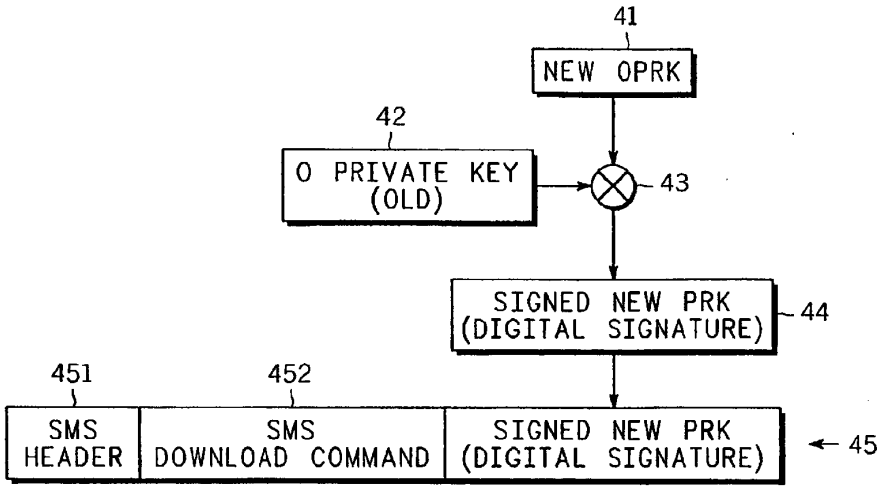
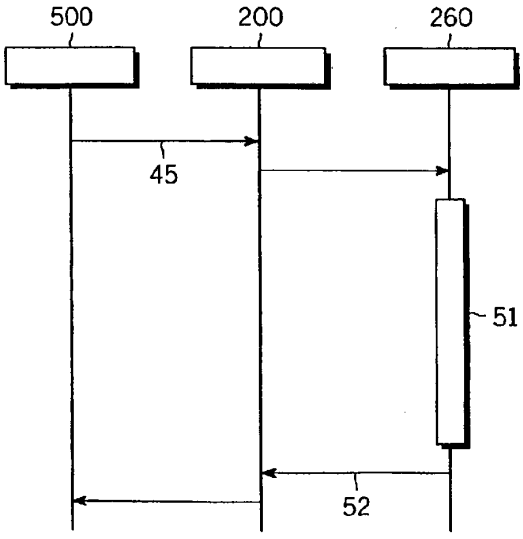


FIG. 4

FIG. 5



BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 444

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 40 2259

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 6 124 799 A (PARKER JOHN PATRICK) 26 September 2000 (2000-09-26) * the whole document *	1-4,6-9	H04Q7/32
X	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29 September 1993 (1993-09-29) * column 4, line 30 - column 5, line 32 *	1,6	
A	EP 1 124 401 A (LUCENT TECHNOLOGIES INC) 16 August 2001 (2001-08-16) * paragraphs '0002!-'0019! * * abstract; claims 1-13 *	2-4,7-9	
A	EP 0 977 452 A (LUCENT TECHNOLOGIES INC) 2 February 2000 (2000-02-02) * the whole document *	2-4,7-9	
A	EP 0 463 384 A (CIT ALCATEL) 2 January 1992 (1992-01-02) * the whole document *	1,6	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 February 2002	Coppieters, S

CATEGORY OF CITED DOCUMENTS

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

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

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 445

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 40 2259

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.

22-02-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6124799 A	26-09-2000	US 5864757 A	26-01-1999
		AU 715488 B2	03-02-2000
		AU 1409997 A	03-07-1997
		CA 2239550 A1	19-06-1997
		EP 0867099 A2	30-09-1998
		JP 11501182 T	26-01-1999
		JP 3080409 B2	28-08-2000
		WO 9722221 A2	19-06-1997
EP 0562890 A	29-09-1993	AT 193965 T	15-06-2000
		DE 69328847 D1	20-07-2000
		DE 69328847 T2	07-12-2000
		EP 0562890 A1	29-09-1993
		ES 2149801 T3	16-11-2000
EP 1124401 A	16-08-2001	AU 1828001 A	16-08-2001
		BR 0100191 A	09-10-2001
		CN 1308472 A	15-08-2001
		EP 1124401 A2	16-08-2001
		JP 2001251292 A	14-09-2001
EP 0977452 A	02-02-2000	US 6243811 B1	05-06-2001
		BR 9902942 A	09-05-2000
		CN 1249588 A	05-04-2000
		EP 0977452 A2	02-02-2000
		JP 2000083017 A	21-03-2000
		TW 428409 B	01-04-2001
EP 0463384 A	02-01-1992	FR 2662878 A1	06-12-1991
		AT 135519 T	15-03-1996
		CA 2043290 A1	01-12-1991
		DE 69117814 D1	18-04-1996
		DE 69117814 T2	25-07-1996
		EP 0463384 A1	02-01-1992
		ES 2084726 T3	16-05-1996
		FI 912548 A	01-12-1991
		JP 3054225 B2	19-06-2000
		JP 4233341 A	21-08-1992
		NO 178597 B	15-01-1996
		US 5303285 A	12-04-1994

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____1289326A1_I_>

IPR2025-01572
Apple EX1002 Page 446

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Headwater Research LLC

Application No./Patent No.: 15/287,597 Filed/Issue Date: 10/6/2016

Titled: Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

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: Inventors (Raleigh et al.) To: Headwater Partners I LLC

   The document was recorded in the United States Patent and Trademark Office at

   Reel 040415, Frame 0879, 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 041268, Frame 0108, or for which a copy thereof is attached.

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.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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 displays a valid OMB control number.

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.

/James E. Harris/	2017-03-21
Signature	Date
James E. Harris	40013
Printed or Typed Name	Title or Registration 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. 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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
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 displays a valid OMB control 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(c).

I hereby appoint:

☒ Practitioners associated with 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 assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) 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
1011 Pruitt Place
Tyler, TX 75703 (USA)

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be Filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, 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	January 3, 2017
Name	David R. Johnson	Telephone	650-517-2782
Title	Chief Financial Officer		

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.

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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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 Patent Application Fee Transmittal	
Application Number:	15287597
Filing Date:	06-Oct-2016
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP041D1C1
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	70	70
UTILITY SEARCH FEE	2111	1	300	300
UTILITY EXAMINATION FEE	2311	1	360	360
Pages:				
UTILITY APPL SIZE FEE PER 50 SHEETS >100	2081	2	200	400
Claims:				
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
LATE FILING FEE FOR OATH OR DECLARATION	2051	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
		Total in USD ($)		**1900**

Electronic Acknowledgement Receipt	
EFS ID:	28698166
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	21-MAR-2017
Filing Date:	06-OCT-2016
Time Stamp:	19:04:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$1900
RAM confirmation Number	032217INTEFSW00006031505876
Deposit Account	505876
Authorized User	Ann Taylor
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)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	P041D1C1_Ext.pdf	163959 bda3e60555d160cd8fc7a99743e2a40071737ec0	no	2
Warnings:					
Information:					
2	Applicant Response to Pre-Exam Formalities Notice	P041D1C1_NFMP.pdf	71875 115ae702525dd91db3a6dd21f4dccb4044cee8f5	no	2
Warnings:					
Information:					
3	Transmittal Letter	P041D1C1_IDSTransLtr.pdf	59067 c7a3df7d5d5c779055cf9a2492a726cdca7569ca	no	2
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	P041D1C1_IDS1.pdf	623011 b2aa7b6e898810b62616337604d05f8068949fea	no	37
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	P041D1C1_IDS2.pdf	621358 98b177daef53845d0d14807892988cad68f9fea8	no	33
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	P041D1C1_IDS3.pdf	621541 a4cd737afd46589ac16f3b5839d477bb74fae3f9	no	33
Warnings:					
Information:					

7	Information Disclosure Statement (IDS) Form (SB08)	P041D1C1_IDS4.pdf	619016 ea5c27b8f8d3efbbc177acfdf44aa776f315e5b7	no	31
Warnings:					
Information:					
8	Information Disclosure Statement (IDS) Form (SB08)	P041D1C1_IDS5.pdf	617775 d2cc566fc717d23ef4727157637c08e8fbd030d6	no	21
Warnings:					
Information:					
9	Foreign Reference	2091.pdf	4030163 9f5a695d3972f432ff9791f8b2ac99ef7cbca74d	no	16
Warnings:					
Information:					
10	Foreign Reference	2092.pdf	2382529 5c57dc228f491cd9301830aad5e4493f4c99b261	no	12
Warnings:					
Information:					
11	Assignee showing of ownership per 37 CFR 3.73	P041D1C1_373Stmt.pdf	121085 90ab16820c8e6b5099445fecfba50ec076b6f0eb	no	3
Warnings:					
Information:					
12	Power of Attorney	HWR_POA.pdf	1117158 29f7900a48aab77b08ab016fed0337e3ae5a66d0	no	2
Warnings:					
Information:					
13	Fee Worksheet (SB06)	fee-info.pdf	42540 4f06b84c16a0066ce4f46610a8600d1afef9ccd8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	11091077		

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.

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. 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 displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): RALEP041D1C1

Application Number: 15/287,597

Filed: October 6, 2016

For: Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

Art Unit: 2447

Examiner: not yet assigned

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.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 700
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ 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.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 505876.

☑ Payment made via EFS-Web.

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.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 40013.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/James E. Harris/ — Signature

March 21, 2017 — Date

James E. Harris — Typed or printed name

903-201-6212 — Telephone Number

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*.

☐ * Total of _____ forms are submitted.

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: Mail Stop PCT, 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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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

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
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1

CONFIRMATION NO. 4727

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

POA ACCEPTANCE LETTER

OC000000090086222

Date Mailed: 03/24/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 03/21/2017.

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**.

/dnguyen/

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
15/287,597	10/06/2016	2447	1200	RALEP041D1C1	1	1

CONFIRMATION NO. 4727

UPDATED FILING RECEIPT

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

OC000000090086645

Date Mailed: 03/24/2017

Receipt is acknowledged of this non-provisional 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 APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Inventor(s)

Gregory G. Raleigh, Woodside, CA;
Jeffrey Green, Sunnyvale, CA;
James Lavine, Corte Madera, CA;

Applicant(s)

Headwater Partners I 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 14/340,270 07/24/2014 PAT 9491199
which is a DIV of 13/309,463 12/01/2011 PAT 8793758
which claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/550,906 10/24/2011
and is a CIP of 13/237,827 09/20/2011 PAT 8832777
and is a CIP of 13/134,028 05/25/2011 PAT 8589541
and is a CIP of 13/253,013 10/04/2011 PAT 8745191
and said 13/237,827 09/20/2011
claims benefit of 61/384,456 09/20/2010
and is a CIP of 12/695,019 01/27/2010 PAT 8275830

IPR2025-01572
Apple EX1002 Page 461

which claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028 05/25/2011
claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/407,358 10/27/2010
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and said 12/694,455 01/27/2010
claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
claims benefit of 61/252,153 10/15/2009
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/134,005 05/25/2011
is a CIP of 12/380,778 03/02/2009 PAT 8321526
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/253,013 10/04/2011
claims benefit of 61/389,547 10/04/2010
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and said 12/695,020 01/27/2010
claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 12/694,445 01/27/2010
claims benefit of 61/252,151 10/15/2009
and said 12/380,778 03/02/2009
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
and said 12/380,780 03/02/2009
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

IPR2025-01572
Apple EX1002 Page 462

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: 10/19/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/287,597**

Projected Publication Date: 06/29/2017

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****
Title

Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

Preliminary Class

709

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 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

IPR2025-01572
Apple EX1002 Page 463

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 AssetsControl, 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

IPR2025-01572
Apple EX1002 Page 464

technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

IPR2025-01572
Apple EX1002 Page 465

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 15/287,597

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	1 minus 20=	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 210 =	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).			400			
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	1130		TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	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.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Gregory G. Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	6219786	B1	2001-04-17	Cunningham et al.	

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	20060020787	A1	2006-01-26	Choyi et al.	
	2	20060072550	A1	2006-04-06	Davis et al.	
	3	20060190987	A1	2006-08-24	Ohta et al.	
	4	20080077705	A1	2008-03-27	Li et al.	
	5	20080259924	A1	2008-10-23	Gooch et al.	

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

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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	2005053335	WO	A1	2005-06-09	Nokia Corp.		

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		

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

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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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	/James E. Harris/	Date (YYYY-MM-DD)	2017-05-10
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 June 2005 (09.06.2005)

PCT

(10) International Publication Number
WO 2005/053335 A1

(51) International Patent Classification[7]: H04Q 7/32

(21) International Application Number:
PCT/EP2004/013101

(22) International Filing Date:
19 November 2004 (19.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/724,569 26 November 2003 (26.11.2003) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ENGELS, Ralf** [DE/DE]; Im Mittelbühl 26, 89160 Dornstadt (DE).

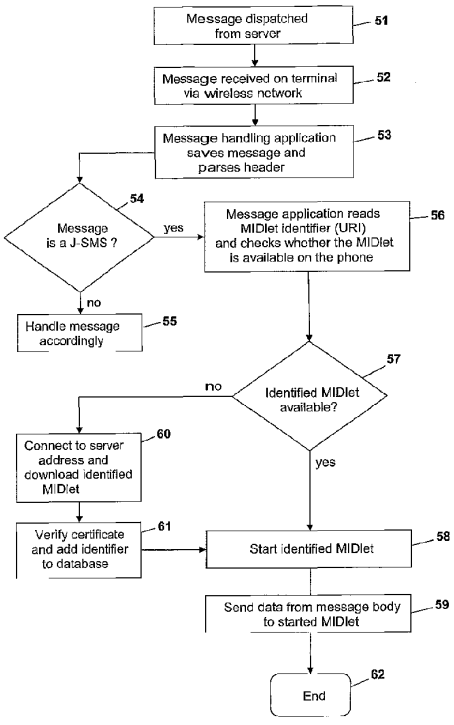
(74) Agent: **VAN WALSTIJN, B., Gerard, G.**; Walstijn Intellectual Property ApS, Parkovsvej 3, DK-2820 Gentofte (DK).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, 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,

[Continued on next page]

(54) Title: FLEXIBLE MESSAGING SYSTEM



(57) Abstract: A universal messaging system for wireless networks that can handle a great variety of different content. The messaging system operates with messages that include an application identifier in the header for an application in platform independent code. The message body contains data to be used by the identified application. The mobile terminals for operation on the wireless network are provided with native software and with a virtual machine capable of executing platform independent code. The identifier allows the mobile terminal to start the correct application for using the data contained in the message body. A uniform recourse identifier (URI) is used to identify the application and to provide an address at which the application can be downloaded if it is not yet available on the message receiving mobile terminal.

WO 2005/053335 A1

IPR2025-01572
Apple EX1002 Page 471

FR, GB, GR, HU, IE, IS, IT, LU, 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).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

FLEXIBLE MESSAGING SYSTEM

The present invention relates to the use of messaging for sending and receiving various items in a wireless communication network.

BACKGROUND ART

Smart Messaging is a concept developed by Nokia for sending and receiving ring tones, picture messages, operator logos, business cards, calendar requests, and Internet settings over the Short Message Service (SMS). Since its introduction in 1997, Smart Messaging has become an extremely popular terminal-specific content delivery technology and the de facto standard for the industry. Examples of different SMS type messages are: Business Card format, Calendar format, Ringing tone format, OTA Bitmap format, CLI Icon format, Operator logo format, Picture Message format and Downloadable Profile message format. There are advanced message types that allow e.g. a network operator to send a complex set of configuration information like "GPRS settings" to a mobile phone. The software on the phones presently on the market is programmed to handle, on average, about 6 to 8 of these different message types. The message types that a phone can handle is determined by the manufacturer, depending on the target customer group, since it is not realistic to attempt to provide a phone that can handle all available message types.

There is presently a fast increase in the number of applications for mobile phones, such as e.g. background images, screen savers, location based services, financial services, operator controlled updating or settings/phonebook contents, etc. that have created a need to increase in the number of message types. It is

CONFIRMATION COPY

IPR2025-01572
Apple EX1002 Page 473

however problematical to harmonize these message types between the different phone manufacturers, despite the dominance of the Nokia Smart Messaging Concept. The present SMS standard may be augmented as described below to provide for more flexible handling of increasing demand.

Accordingly, a need exists for a universal messaging system for wireless networks that can handle a great variety of different content.

DISCLOSURE OF THE INVENTION

The devices and method described below provide for a method of handling incoming messages received on a mobile communication terminal via a wireless network, the terminal having native software and a virtual machine capable of executing applications in platform independent object code. The method comprises the step of receiving and storing a message that comprises a header and a message body. The header contains an identifier for an application in platform independent object code to be executed by the virtual machine. In the next step it is verified if the identified application is available on the terminal, and the identified application is started when available on the terminal.

Thus, the terminal is able to automatically start the application required for using the data in the message body of a received message, regardless of the type and version of the native software of the terminal unless the required application is not available on the terminal. Therefore, the header may further contain an address at which the identified application can be downloaded from a server that is accessible through the wireless network, and the method further comprises the steps of connecting

IPR2025-01572
Apple EX1002 Page 474

to the terminal to the server at the address contained in the header, downloading the identified application when the identified application was not available on the terminal, and starting the identified application when downloaded.

Thus, the required application can automatically be downloaded if it is not already available on the terminal. Since the application is in platform independent object code, there is no platform compatibility problems, and because the download address is contained in the header the user does not need to search for it.

Preferably, the message body contains data to be used by the identified application.

The platform independent object code can be Java™, in particular Java™ 2 Platform, Micro Edition (J2METM) from Sun Microsystems Inc. but other platform independent object codes can be used.

The virtual machine preferably is a K Virtual Machine™ (KVM). The identified application can be a Java™ application, a Java™ applet or a Java™ MIDlet.

The devices and method described below provide for a mobile communication terminal that can operate with a flexible messaging concept for a wireless network. This terminal has native software and a virtual machine. The virtual machine is capable of executing applications in platform independent object code. The terminal also has a message handling application in the native software or in an application run by the virtual machine. The message handling application is capable of sending and receiving messages via the wireless network, and the

IPR2025-01572
Apple EX1002 Page 475

message handling application is programmed to start an application written in the independent object code when a corresponding identifier is contained the header of a received message.

Thus, the terminal is able to automatically start the application required for using the data in the message body of a received message, regardless of the type and version of the native software of the terminal if the required application is available on the terminal.

The message handling application can also be programmed to download the identified application from a server that is accessible via the wireless network at an address contained in the header when the identified application is not already available on the terminal.

The message handling application is programmed to verify the certification of the downloaded application.

The mobile communication terminal may further comprise an application identifier database listing the identifiers of all the applications in platform independent object code that are available on the terminal.

The message to be used with a flexible messaging concept for mobile terminals that operate on a wireless network is describe in detail below, and provides a format suitable for transmission through a wireless network to a mobile communication terminal, the terminal having native software and an virtual machine capable of handling platform independent object code and the message having a syntax comprising a header part and message body part. The header contains an identifier for an application in platform independent object code to be executed by the

IPR2025-01572
Apple EX1002 Page 476

virtual machine in the mobile communication terminal that receives the message.

Preferably, the header includes an address at which the identified application can be downloaded from a server that is accessible through the wireless network. The message body may contain data to be used by the identified application.

The message header may include a URI that serves as identifier and contains the address at which the identified application can be downloaded from a server.

The message can be an SMS message with a port address in octets 4-5 that identifies it as a message containing an identifier for an application in platform independent object code to be started upon receipt of the message. The identified application can be a Java™ applet or MIDlet, preferably in the Java™ 2, Micro Edition, Mobile Information Device Profile (MIDP) format.

The message may also contain a signed certificate issued by a recognized certification authority and including a public key from the signatory. In addition, the message may include field communication of an unique sender identifier in the form of a telephone number of an originating mobile phone, or other unique identifier for mobile terminals and/or computers.

On this background, it is an object of the present invention to provide.

With the system described herein, a flexible messaging method for mobile terminals that operate on a wireless network achieved by providing a method of enabling an application in platform independent object code to be run

IPR2025-01572
Apple EX1002 Page 477

on a mobile communication terminal comprising the steps of sending a message from a server via the wireless network to a mobile communication terminal, the terminal being provided with a virtual machine capable of executing applications in platform independent object code. The message contains a header with an identifier for the application to be started on the mobile communication terminal and a message body with the data to be used by the identified application.

Thus, the system and methods described herein make it possible to send a message with data to be used by a specific application to a mobile communication terminal, without needing to know first which platform is installed in the terminal.

The message header may further contain an address at which the identified application can be obtained from a server that is accessible through the wireless network, and thus the method may further comprise the step of uploading the identified application to the mobile communication terminal when the mobile terminal connects to the server at the address in the header.

Thus, it is rendered possible to transfer an application to a mobile terminal without being required to know the platform installed on the terminal. There is also no risk of installing the application twice on the same terminal.

Further objects, features, advantages and properties of the flexible messaging system according to the invention will become apparent from the detailed description.

IPR2025-01572
Apple EX1002 Page 478

BRIEF DESCRIPTION OF THE DRAWINGS

In the following detailed portion of the present description, the invention will be explained in more detail with reference to the exemplary embodiments shown in the drawings, in which

Fig. 1 shows the architecture of a wireless cellular communication network for use with the present invention,
Fig. 2 shows a mobile phone in accordance with the present invention,
Fig. 3 is a block diagram showing the basic components of the mobile phone of Fig. 2,
Fig. 4 shows the software architecture of the mobile phone of Fig. 2,
Fig. 5 is a flowchart illustrating the message handling procedure according to a preferred embodiment of the present invention,
Fig. 6 shows a sequence diagram of an example of the use of the flexible messaging system according to the invention, and
Fig. 7 shows a sequence diagram of a further example of the use of the flexible messaging system according to the invention.

DETAILED DESCRIPTION

Fig. 1 illustrates a network architecture for use with the present invention. The telecommunication system includes a wireless cellular network 16 and a data network 24. The wireless cellular network 16 can be implemented in a conventional wireless cellular telephone network that has been enhanced to carry data. A wireless network capable of carrying circuit-switched data can be used for this purpose. More preferably, however, the wireless cellular network provides a packet-switched data

IPR2025-01572
Apple EX1002 Page 479

service. An example of a wireless infrastructure includes UMTS (Universal Mobile Telephone System), a 3rd Generation wireless system based on GSM (Global System for Mobile communications). GSM adds a packet network overlay known as GRPS (GSM Packet Radio Service) to a wireless circuit voice network. The data network can e.g. be the Internet.

The cellular network comprises a large number of base stations 20 (only two are shown) that are provided with a transceiver for handling mobile phone communications. The base stations 20 are connected to a mobile switching centre 21. Each of the base stations 20 has its own control channel frequency (control channel frequencies can be reused for distant cells).

The base stations 20 are provided with an SMS/MMS message controller (not shown) and an SMS/MMS message transmission driver to allow it to send message to a mobile phone 1 and to receive messages from a mobile phone 1.

The mobile switching centre 21 is connected to a data 22 switching node that connects the cellular communication network 16 with the data network 24. Different servers 25,26,27,28 described in more detail below, are connected to the data network.

Fig. 2 shows a preferred embodiment of a mobile phone 1 according to the invention. The mobile phone 1, comprises a user interface having a keypad 2, a display 3, an on/off button 4 (present in the top of the phone) a speaker 5, and a microphone 6 (only the opening present in the bottom of the phone is visible). The mobile phone 1 according to the preferred embodiment is adapted for communication via a cellular network, such as the GSM

IPR2025-01572
Apple EX1002 Page 480

900/1800 MHz network, but could just as well be adapted for use with a Code Division Multiple Access (CDMA) network.

According to a preferred embodiment, the keypad 2 has a first group 7 of keys as alphanumeric keys, two softkeys 9, a cursor navigation key 10 (scroll up/down), and on-hook and off-hook keys 12. The present functionality of the softkeys 9 is shown in separate fields (softkey-labels) in the display 3 just above the softkeys 9. The softkeys 9 are multifunction keys and their present function depends on the state of the mobile phone 1. The softkeys 9 give access to the menu, the phonebook and call can activate actions related to call handling and message handling. A releasable battery pack 14 is placed on the rear side of the mobile phone 1.

Fig. 3 schematically shows the most important components of a preferred embodiment of the mobile phone 1, said components being essential to the understanding of the invention. The processor 18 controls the communication with the network via the transmitter/receiver circuit 19 and an internal antenna 15.

The microphone 6 transforms the user's speech into analogue signals, the analogue signals formed thereby are A/D converted in an A/D converter (not shown) before the speech is encoded in a digital signal processing unit 14 (DSP). The encoded speech signal is transferred to the processor 18, which i.e. supports the GSM terminal software. The processor 18 also forms the interface to the peripheral units of the apparatus, including a RAM memory 17a and a Flash ROM memory 17b, a SIM card 16, the display 3 and the keypad 2 (as well as data, power supply, etc.). The DSP 14 speech-decodes the signal,

IPR2025-01572
Apple EX1002 Page 481

which is transferred from the processor 18 to the speaker 5 via a D/A converter (not shown).

Fig. 4 illustrates the software architecture of the mobile phone 1. The software architecture comprises an operating system, in a preferred embodiment the Symbian™ 7.0 OS that provides the platform for the native software. The native software comprises a number of native applications of which a few can be mentioned: User interface, KVM support, a call handling, phone book, message handling and a MIDlet database. The listed native applications are, however, merely exemplary, there could be more as well as fewer native applications.

A Connected Limited Device Configuration (CLDC) provides the runtime environment for Java™ applications. CLDC is one of the most appropriate configurations for mobile phones available for Java™, since it is tailored for devices with 160-512 KB memory battery powered, slow, possibly intermittent, connection.

The CLDC comprises a K Java™ Virtual Machine (KVM) and a set of libraries and Application Program Interfaces (APIs). The libraries and APIs are specified in the Mobile Information Device Profile (MIDP) sitting on top of the CLDC. The MIDP is a vertical extension of CLDC. Together they provide a run-time environment for Java™ Applets and MIDlets (MIDlet: an application written for the Mobile Information Device profile (MIDP)) on the mobile phone concerned.

The MIDlets are in code that is created by a Java™ compiler. This code can be run on any platform that has a KVM installed. A MIDlet will run the same in any KVM, regardless of the hardware and software underlying the system. The MIDLETS are therefore ideal for extending

IPR2025-01572
Apple EX1002 Page 482

the functionality of mobile phones, also because their relatively small size renders them suitable for downloading to the phone. In the present embodiment, a calculator MIDlet and two other MIDlets X2 and X3 have been downloaded to the mobile phone 1. The MIDlets co-exist with other applications on the mobile phone 1 such as the Original Equipment Manufacturer (OEM) Specific Applications. In the present embodiment a Java™ xhtml micro browser applet has been installed by the OEM.

The message handling application is capable of receiving, creating and sending text messages in the SMS standard (Short Message Service (SMS) part of the Global System for Mobile communications (GSM) digital standard - well known in the art). The message handling application may also be able to handle other message formats for exchanging information between mobile phones/servers such as the more recent MIME (Multipurpose Internet Mails Extensions) and MMS (Multimedia Messaging Service) standards. The message handling application may run in the native software or in an application run by the virtual machine.

The mobile phone 1 can send and receive data using the General Packet Radio Service (GRPS) for e.g. downloading MIDlets or other applications and is Wireless Application Protocol (WAP) enabled. A micro-browser written in Java™ is one of the OEM-specific applications.

The present invention provides for a new SMS message type in which the message header contains a MIDlet identifier and an address at which the identified MIDlet can be downloaded from a server that is connected to the wireless cellular network. This header is in addition the now-standard SMS header and the user data header. The message body contains the data to be used by the

IPR2025-01572
Apple EX1002 Page 483

identified MIDlet. The new SMS message type will be referred to hereafter as a Java-message (J-SMS).

The syntax of the J-SMS in a preferred embodiment is as follows:

<sms>::=

<sms-header>

<sms-data>

<sms-header>::= standard sms header described somewhere else

<sms-data>::

<user-data-header>

<user-data>

<user-data-header>::= user data header as described in smart messaging specification

<user-data>::=

<j-sms-header>

<j-sms-data>

<j-sms-header>::=

<j-sms-header-length>

<j-sms-version>

<j-sms-flags>

<j-sms-uris>

<j-sms-certificates>

<j-sms-header-length>::=two bytes giving the length of the j-sms header

<j-sms-version>::=one byte with the version of the j-sms protocol (01)

<j-sms-flags>::=one byte with flags for the message. Sum of the following:

IPR2025-01572
Apple EX1002 Page 484

1: the message includes certificates and a checksum

2: the message can be displayed as text

4: the message can be discarded if not able to display

<j-sms-uris>::=

<number of uris>

*<uri_s>**

<number of uris>::=one byte with the number of uris

<uri_s>::=uri's terminated with \n

<j-sms-certificates>

<checksum>

*<certificate>**

<checksum>::=checksum of the whole user data block (user data header plus user data) excluding this checksum

<certificate>::=certificate in base64 encoding terminated by \n

<j-sms-data>::=data that is to be transferred to the MIDlet

An example of a J-SMS in accordance with a preferred embodiment of the present invention in the form of an application port addressing scheme as defined in GSM 03.40 is listed below:

Octet Number	Value	Description
1	0B	Length of the User Data Header
2	05	Information Element Identifier (IEI; application port addressing scheme, 16-bit port address)
3	04	Information Element Data Length (IEDL)
4 - 5	2136	Information Element Data (octets 4 & 5 → 2136 - destination port)

IPR2025-01572
Apple EX1002 Page 485

6 - 7	00 00	Information Element Data (octets 6 & 7 → 0000 - originator port)
8	00	Information Element Identifier (IEI; concatenated short message, 8-bit reference number)
9	03	Information Element Data Length (IEDL; 3 octets)
10	01	Information Element Data (concatenated short message reference number)
11	02	Information Element Data (total number of concatenated messages (0-255))
12	01	Information Element Data (sequence number of current short message)
13	30	MIDlet message version number. ISO-8859-1 character "0"
14	00	Message flags where the following bits have the meaning: 1. message includes certificate 2. message data can be displayed as text 3. message can be discarded if not able to display 4. reserved for future use.
15	01	Number of following URIs
16..	"http://www.d2.de/greetingcard.jat"	The URI of the MIDlet used to display the content. Terminated by a newline (0x0A) character.
..	http://www.d2.de/greeting/picture1.jpg "Hi there, how are you doing ?".	MIDlet message data in a format defined only by the MIDlet.

The port number in octet 4-5 defines the SMS message type. The number used in this example is arbitrary and has not been reserved for the message type according to the present invention. Regular port numbers are reserved in the NBS port number space at the Internet Assigned Numbers Authority (IANA).

IPR2025-01572
Apple EX1002 Page 486

Octets 1 to 12 are in use in conventional SMS types, and for further information on their function reference is made to the GSM 03.40 specification, hereby incorporated by reference.

Octet 13 identifies the MIDlet message version number.

Octet 14 contains message flags where the following bits have the meaning:

1. message includes certificate
2. message data can be displayed as text
3. message can be discarded if not able to display
4. reserved for future use.

Octet 15 defines the number of Uniform Resource Identifiers (URIs) contained in the message. Octet 16 contains the first URI, followed by the message body with the data to be used by the identified MIDlet.
The message handling application detects the message type through the port number in octet 4-5. If the port number is (in present example) 2136 (HEX) the message is treated as a J-SMS. SMS messages with other port numbers in octet 4-5 are handled by the message handling application in the respective intended way, which is though not described here since this other types of the message handling are well known from e.g. the SMART MESSAGING SPECIFICATION, Revision 3.0.0, 2000-12-18, hereby incorporated by reference.

The MIDlet to be executed upon receipt of the message is defined by the URI in octet 16. The data to be used during the execution of the identified MIDlet is contained in the message body in the following octets. The data may comprise image files, formatted text files, audio files database files, or any other type of file executable on the terminal, or it may contain links to

IPR2025-01572
Apple EX1002 Page 487

such files. Referring to the table, greeting card MIDlet identified in octet 16 is needed to display the greeting card which includes an image file and associated text. The greeting card image file "picture1.jpg" is provide by an identification of the URI "http://www.d2.de/greeting/picture1.jpg," and the accompanying text "Hi there, how are you doing?" is provided as a text file within the message itself.

The following example illustrates the practical application of the J-SMS type messages. A first mobile subscriber A wishes to send his friend, mobile subscriber B, an e-postcard. Subscriber A visits the WAP-site of a postcard server 25 using the micro browser on his mobile phone 1. There, he selects the type of e-postcard to be sent, e.g. the graphics, accompanying tune, animation, font type, color, etc. The server 25 prompts subscriber A to enter a message text, that may or may not be used in combination with text integrated in the selected e-postcard. The server 25 also prompts subscriber A to enter the intended recipient's name and phone number. When the server 25 has received these data and an accept from subscriber A it sends a J-SMS to subscriber B. The header of the J-SMS contains an identifier for a postcard displaying MIDlet, and an address where the postcard displaying MIDlet can be downloaded from a server, in this case a MIDlet server 26, but it could just as well have been the postcard server 25. The URI serves as MIDlet identifier and as download address.

The postcard displaying MIDlet is an application that displays the postcard as selected and composed by subscriber A correctly on any mobile device with a Java™ Virtual Machine. The postcard contains text and may contain graphics, backgrounds, animations, music, etc.

IPR2025-01572
Apple EX1002 Page 488

The message body contains the data for the postcard displaying MIDlet.

Fig. 5 is a flowchart that illustrates the procedure after dispatch of the J-SMS (step 51). Upon receipt of the J-SMS by the mobile phone 1 of subscriber B (step 52) the message handling application saves the message and examines the message header (step 53), parsing the message header for the information indicated in table above. Then, the message handling application determines the message type by checking the port number in octets 4-5 (step 54).

If the message is not a J-SMS, but e.g. a profile or a text message, the message handling application handles the message accordingly (step 55), as is well-known in the art and therefore not further explained here.

If the message handling application finds port number 2136 (HEX) in octet 4-5 the message is handled as a J-SMS. The message handling application reads the first URI included in the message. The URI serves as the MIDlet identifier. The mobile phone 1 maintains a small MIDlet database (one of the native applications) that lists the URIs of all the MIDlets that have been downloaded to the phone. The URI of OEM installed MIDlets is preferably also listed in the MIDlet database. The message handling application checks the MIDlet database for the presence of the URI included in the header (step 56).

After checking the MIDlet database, the message handling application can determine (step 57) if the identified MIDlet, in this example the postcard displaying MIDlet, is available on the mobile phone 1.

IPR2025-01572
Apple EX1002 Page 489

If the identified MIDlet is available, the message handling application starts the postcard displaying MIDlet (step 58). The message handling application then sends the data in the message body to the postcard displaying MIDlet (step 59) which uses it to display the postcard as selected and composed by subscriber A, including the image on the picture1.jpg file and the personal text "Hi there, how are you doing?" (step 59A in Figure 5).

If the URI identified MIDlet was not found in the MIDlet database in step 56, the message handling application connects e.g. via GPRS to the address in the URI at which the identified midlet can be downloaded and downloads the identified MIDlet. In this example the postcard displaying MIDlet is downloaded from the MIDlet server 26 (step 60). In the download request the message handling application may provide information about the requesting phone. The MIDlet sever 26 uploads the postcard handling MIDlet to the mobile phone 1.

Next, the message handling application adds the URI of the downloaded MIDlet to the MIDlet database and verifies that the certificate accompanying the MIDlet is signed and issued by an recognized certificate authority to ensure the integrity of the MIDlet (step 61).

A certificate issued by a recognized certificate authority is added to the signed MIDlet. The carrier, or the software developer, creates a signing-key pair and obtains a certificate from a recognized certificate authority. The carrier or developer computes a signature of the MIDlet suite JAR, then places that signature and the corresponding certificate in the application descriptor.

IPR2025-01572
Apple EX1002 Page 490

The signed MIDlet suite assures the user that the contents of the MIDlet suite have not been tampered with, and that the MIDlet suite comes from an trusted source. The MIDP implementation on the device can verify the identity of the developer by verifying the developer's signature. It can use the developer's public key added to the Java Application Descriptor (JAD) to verify the integrity of the MIDlet suite itself. For further details on the certification of MIDlets reference is made to the MIDP 2.0 specification (hereby incorporated by reference).

The MIDlet is then handled in accordance with the permission levels indicated in the certificate. The permissions may comprise allowed permissions and user permissions (the ones for which the user will be consulted). The permission levels are stepped in the following order: Network operators (highest level), OEM (mid level), signed but not by Network operator or OEM (lowest level). Depending on these levels the phone prompts for permission for sensitive operations to e.g. opening an HTTP connection, to delete or change phone numbers, etc.

After the certificate verification the message handling application starts the postcard displaying MIDlet (step 58), sends the data in the message body to the postcard displaying MIDlet (step 59) and the postcard is displayed.

The procedure can be repeated if subscriber B replies by sending an e-postcard back to subscriber A, a function that may be built into the postcard displaying application. Otherwise, the message handling application ends in step 62.

IPR2025-01572
Apple EX1002 Page 491

There can be more than one MIDlet identifier (URI) included in a single J-SMS. The message application will execute the identified MIDlets in the order in which they are listed in the J-SMS. In the above example the URI has been used both to identify the MIDlet and to provide the address at which the MIDlet can be downloaded. It is however possible to use a separate identifier and address. The MIDlet that is started by the J-SMS may also download further information or other data.

Another example of the use of the present invention is illustrated in Fig. 6 with the following scenario. An e-mail provider wishes to send e-mail messages to mobile subscribers. The standard SMS e-mail message is not sufficient for the operator's requirements because more features should be implemented e.g. starting an xhtml browser to read the e-mail, displaying the header of the new received e-mail, displaying the provider logo, showing an in-tray with received e-mails in every user's e-mail folder. After receipt of an e-mail intended for a mobile subscriber, the operator's e-mail server 27 sends a J-SMS that starts a MIDlet that displays the text "e-mail received" on the display of the mobile phone together with an audible notification and prompts the user if the e-mail should be opened. If the user affirms but the required enhanced e-mail MIDLET (an xhtml Java™ browser) is not installed on the user's mobile phone, the mobile phone requests a download of the enhanced e-mail MIDlet from the URI listed in the e-mail message, processes the download to install the enhanced e-mail MIDLET, and thereafter executes the enhanced e-mail MIDLET to process the e-mail data. The xhtml browser exchanges e-mail data via GPRS between the mobile phone 1 and the e-mail server 27 and displays the e-mail data. The xhtml browser operates as a sophisticated e-mail client that offers the user more flexibility and comfort

IPR2025-01572
Apple EX1002 Page 492

than the simple e-mail displaying capacities of conventional SMS. The steps of requesting the MIDlet from the MIDlet server and the subsequent download as shown in Fig. 6 are bypassed if the xhtml browser MIDlet is already available on the mobile phone 1.

A further example of the use of the present invention is illustrated in Fig. 7 with the following scenario. A network operator wishes to offer a new service to its customers. This new service sends special offers from the operator's web-shop to the mobile phone of the customers. This service is realized by the provider sending J-SMSs including name, price and description (photo) of the offered items from its web-shop server (e.g., block 28 of Figure 1). The J-SMS includes an identifier of an advertisement displaying MIDlet that displays this information in a clean way, stores past offers for reference and allows the subscriber to order the items at the web-shop. The steps of requesting the MIDlet from the MIDlet server and the subsequent download as shown in Fig. 7 are bypassed if the advertisement displaying MIDlet is already available on the mobile phone 1.

The integrity verification does not need to be exclusively applied to the MIDlets, it can also be implemented in the J-SMS itself by adding a certificate from a recognized certificate authority and an encrypted checksum of the whole message to the J-SMS. The validity of the certificate can be verified by opening the signature with the public key that is included in the J-SMS. In this embodiment of the J-SMS the verification can be carried out before downloading the MIDlet concerned. Thus, some unnecessary downloads of uncertified MIDlets can be avoided.

IPR2025-01572
Apple EX1002 Page 493

As illustrated above, the messaging system provides a message format for use in a mobile phone system wherein mobile phones are capable of running a variety of applications to process a variety of files, and are capable of running a message handling application for receiving messages. The message format comprises a header portion for identifying the message to the message handling application and a message data portion. The message data portion further comprises (1) a message data file portion which may optionally contain message text files, message images, message audio, message database files or the like, or identification of message files and locations from which said message files or the like may be downloaded to the phone, as desired by the originator of the message and (2) a message data header portion which contains an identification for any application needed in order to process files contained or identified in the message data file portion, and also contains information regarding locations from which said application may be downloaded to the phone. In addition, the message format may comprise a user data header according the SMS specification, and various other headers as dictated by the particular message contents.

Although the present invention has been described in detail for purpose of illustration, it is understood that such detail is solely for that purpose, and variations can be made therein by those skilled in the art without departing from the scope of the invention. The message type is not limited to the SMS standard, and may be implemented in MMS or EMS standards. The applications that are executed after receipt of a message do not need to be MIDlets, they could just as well be Java™ applets or other applications in platform independent code. The platform independent runtime environment does not need to be Java™ based, other runtime environments for platform

IPR2025-01572
Apple EX1002 Page 494

independent code can be used. Thus, while the preferred embodiments of the devices and methods have been described in reference to the environment in which they were developed, they are merely illustrative of the principles of the inventions. Other embodiments and configurations may be devised without departing from the scope of the appended claims.

IPR2025-01572
Apple EX1002 Page 495

CLAIMS:

1. A method of handling incoming messages received on a mobile communication terminal via a wireless network, the terminal having native software and a virtual machine capable of executing platform independent object code, comprising the steps of:

receiving and storing a message that comprises a header and a message body, the header containing an identifier for an application in platform independent object code that can be executed by the virtual machine,

verifying if the identified application is available on the terminal, and

starting the identified application when available on the terminal

2. A method according to claim 1, wherein the header further contains an address at which the identified application can be downloaded from a server that is accessible through the wireless network, and further comprising the steps of:

connecting to the terminal to the server at the address contained in the header and downloading the identified application when the identified application was not available on the terminal, and

starting the identified application when downloaded.

3. A method according to claim 1, wherein the message body contains data to be used by the identified application.

IPR2025-01572
Apple EX1002 Page 496

4. A method according to claim 2, wherein the message body contains data to be used by the identified application.

5. A method according to claim 3, wherein the message body contains greeting card data that is to be used by a greeting card displaying application identified in the header.

6. A method according to claim 4, wherein the message body contains greeting card data that is to be used by a greeting card displaying application identified in the header.

7. A method according to claim 3, wherein the message body contains phone number data that is to be used by a phonebook updating application identified in the header.

8. A method according to claim 4, wherein the message body contains phone number data that is to be used by a phonebook updating application identified in the header.

9. A method according to claim 3, wherein the message body contains e-mail data that is to be used by an e-mail displaying application identified in the header.

10. A method according to claim 4, wherein the message body contains e-mail data that is to be used by an e-mail displaying application identified in the header.

11. A method according to any of claims 1 to 10, wherein the platform independent object code is Java™, preferably in the Java™ 2, Micro Edition format.

12. A method according to any of claims 1 to 10, wherein the virtual machine is a Java Virtual Machine, preferably a K Virtual Machine™ (KVM) .

IPR2025-01572
Apple EX1002 Page 497

13. A method according to any of claims 1 to 10, wherein the identified application is a MIDlet.

14. A method according to any of claims 1 to 10, further comprising the step of verifying the certification of the identified application.

15. A mobile communication terminal for operation with a wireless network, the terminal having:

native software,

a virtual machine capable of executing platform independent object code,

a message handling application in the native software or in an application under the virtual machine, the message handling application being capable of sending and receiving messages via the wireless network, and

the message handling application being programmed to start an application written in the independent object code when a corresponding identifier is contained the header of a received message.

16. A mobile communication terminal according to claim 15, wherein the message handling application is programmed to download the identified application from a server that is accessible via the wireless network at an address contained in the header when the identified application is not already available on the terminal.

17. A mobile communication terminal according to claim 15, wherein the platform independent object code is Java™, preferably in the Java™ 2, Micro Edition format.

IPR2025-01572
Apple EX1002 Page 498

18. A mobile communication terminal according to claim 17, wherein the virtual machine is a Java™ Virtual Machine, preferably a K Virtual Machine™ (KVM).

19. A mobile communication terminal according to any of claims 15 to 18, wherein the identified application is a MIDlet.

20. A mobile communication terminal according to any of claims 15 to 18, wherein the message handling application is programmed to verify the certification of the downloaded application.

21. A mobile communication terminal according to any of claims 15 to 18, wherein the message application is programmed to send the data in the message body to the identified application.

22. A mobile communication terminal according to any of claims 15 to 18, further comprising an application identifier database listing the identifiers of all the applications in platform independent object code that are available on the terminal.

23. A message for transmission through a wireless network to a mobile communication terminal, the terminal having native software and a virtual machine capable of executing applications in platform independent object code, the message having a syntax comprising:

a header part, and

a message body part,

the header containing an identifier for an application in platform independent object code to be executed by the virtual machine on the mobile communication terminal that receives the message.

IPR2025-01572
Apple EX1002 Page 499

24. A message according to claim 23, wherein the header includes an address at which the identified application can be downloaded from a server that is accessible through the wireless network.

25. A message according to claim 23 or 24, wherein the message header contains a URI that serves as identifier and contains the address at which the identified application can be downloaded from a server.

26. A message according to any of claims 23 or 24, wherein the message body contains data to be used by the identified application.

27. A message according to any of claims 23 or 24, wherein the message is an SMS message with a port address in octets 4-5 that identifies it as a message containing an identifier for an application to be started upon receipt of the message.

28. A message according to any of claims 23 or 24, wherein the identified application is a Java™ applet or a MIDlet, preferably in the Java™ 2, Micro Edition, Mobile Information Device Profile (MIDP) format.

29. A message according to any of claims 23 or 24, further containing a signed certificate issued by a recognized certification authority that includes a public key from the signatory.

30. A method of enabling an application in platform independent object code to be run on a mobile communication terminal comprising the steps of:

sending a message from a server via the wireless network to the mobile communication terminal that is provided with a virtual machine capable of executing applications in platform independent object code, the message containing:

IPR2025-01572
Apple EX1002 Page 500

a header with an identifier for the application to be executed by the virtual machine and

a message body with the data to be used by the identified application.

31. A method according to claim 30, wherein the message header further contains an address at which the identified application can be obtained from a server that is accessible through the wireless network, further comprising the step of:

uploading the identified application to the mobile communication terminal when the mobile terminal connects to the server at the address contained in the header.

32. A method according to claim 30, wherein the server that uploads the identified application is not the same as the server sending the message.

33. A method according to claim 30, wherein the uploaded application is a MIDLet, preferably in the Java™ 2, Micro Edition, Mobile Information Device Profile (MIDP) format.

34. A message format for use in a mobile phone system wherein mobile phones are capable of running a variety of applications to process a variety of files, and are capable of running a message handling application for receiving messages, said message format comprising:

a header portion for identifying the message to the message handling application;

a message data portion, said message data portion further comprising;

a message data file portion which may optionally contain message text files, message images,

IPR2025-01572
Apple EX1002 Page 501

message audio, message database files or the like, or identification of message files and locations from which said message files or the like may be downloaded to the phone, as desired by the originator of the message; and

a message data header portion, wherein said message data header portion contains an identification for any application needed in order to process files contained or identified the message data file portion, and also contains information regarding locations from which said application may be downloaded to the phone.

35. A method of transmitting messages to a mobile phone in a mobile phone system wherein mobile phones are capable of running a variety of applications to process a variety of files, and are capable of running a message handling application for receiving messages; said method comprising the steps of:

creating a message in a message format comprising:

a header portion for identifying the message to the message handling application

a message data portion, said message data portion further comprising;

a message data file portion which may optionally contain message text files, message images, message audio, message database files or the like, or identification of message files and locations from which said message files or the like may be downloaded to the phone, as desired by the originator of the message; and

a message data header portion, wherein said message data header portion contains an

IPR2025-01572
Apple EX1002 Page 502

identification for any application needed in order to process files contained or identified the message data file portion, and also contains information regarding locations from which said application may be downloaded to the phone; and

transmitting the message to a mobile phone.

36. A method of operating a mobile phone comprising;

programming the phone to receive messages having a format such that the messages comprise an SMS header portion and an SMS data portion, wherein the SMS data portion comprises a first portion comprising message handling information and a second portion comprising message data for eventual display to the mobile phone user, wherein the message handling information comprises information identifying an application needed to display the message data or otherwise process the message data with an application, and information identifying a location from which the application may be downloaded to the phone; and wherein the message data comprises message files comprising message text files, message images, message audio, message database files or the like, or identification of locations from which said message files or the like may be downloaded to the phone;

further programming the phone to determine if the application needed to display or otherwise use the message data is installed on the phone, and, if not, to download the application from the

IPR2025-01572
Apple EX1002 Page 503

location identified in the message handling information;

further programming the phone to display or otherwise use the message files or the like if they are already in the message data, or, if not, to download the message files from the locations identified in the message data;

operating the phone to receive a message, and thereafter operating the phone to determine if the application needed to use the message files is installed on the phone, and, if not, to download the application; and thereafter operating the phone to display or otherwise use the message files if they are contained in the message data, and, if not, to download the message files from the location identified in the message data and thereafter display or otherwise use the message files.

37. The message format of claim 34 wherein the messages are provided in an SMS format.

38. The message format of claim 34 wherein the messages are provided in an MMS format.

39. The message format of claim 34 wherein the messages are provided in an EMS format.

40. The method of claim 35 or 36 wherein the messages are provided in an SMS format.

41. The method of claim 35 or 36 wherein the messages are provided in an MMS format.

42. The method of claim 35 or 36 wherein the messages are provided in an EMS format.

IPR2025-01572
Apple EX1002 Page 504

43. The message format of claim 34 wherein the message header is an SMS header, and wherein the message format further comprises a user data header.

44. The method of claim 35 further comprising creating the message in a message format comprising a user data header.

45. The method of claim 36 wherein the message header is an SMS header, and wherein the message format further comprises a user data header.

IPR2025-01572
Apple EX1002 Page 505

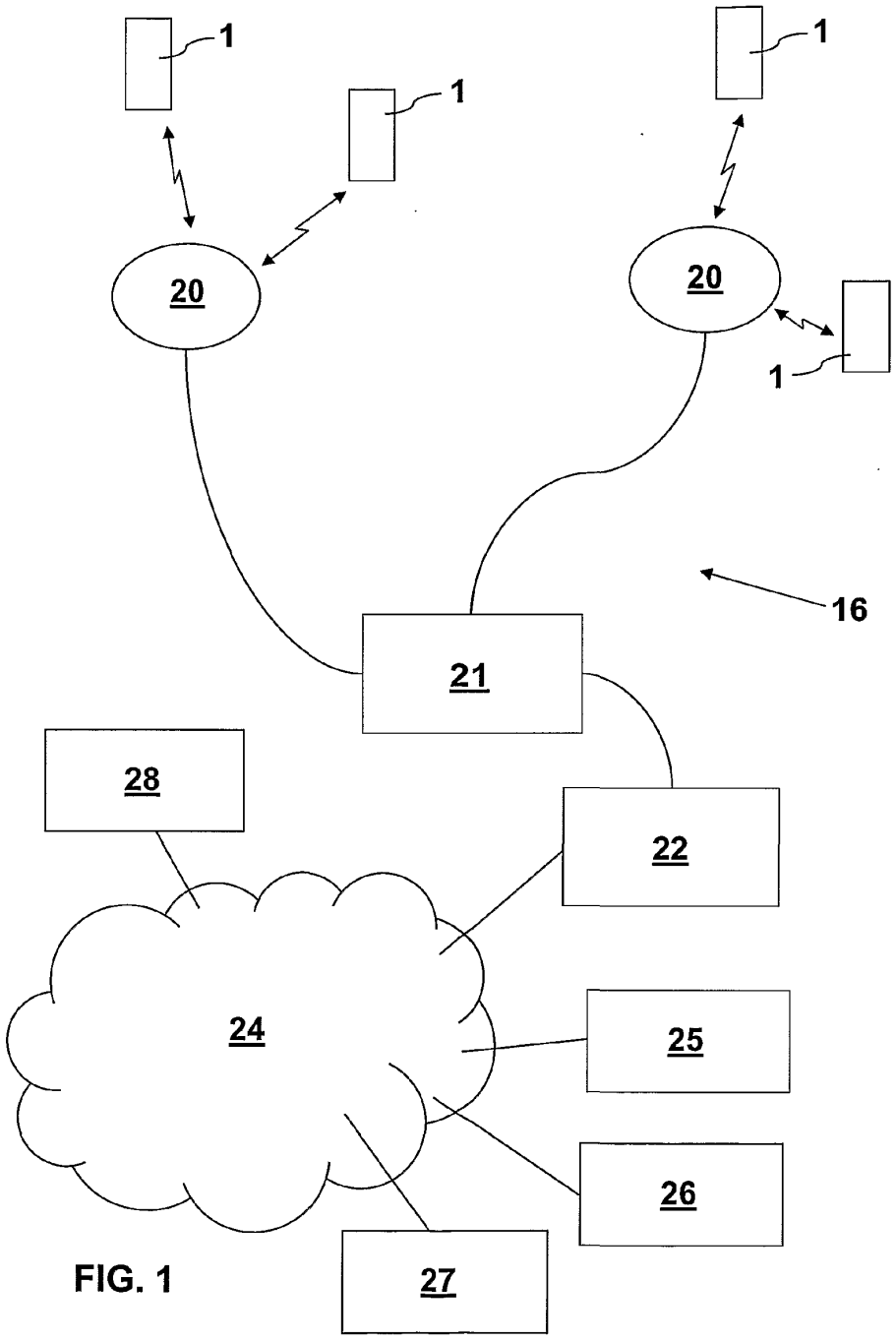


FIG. 1

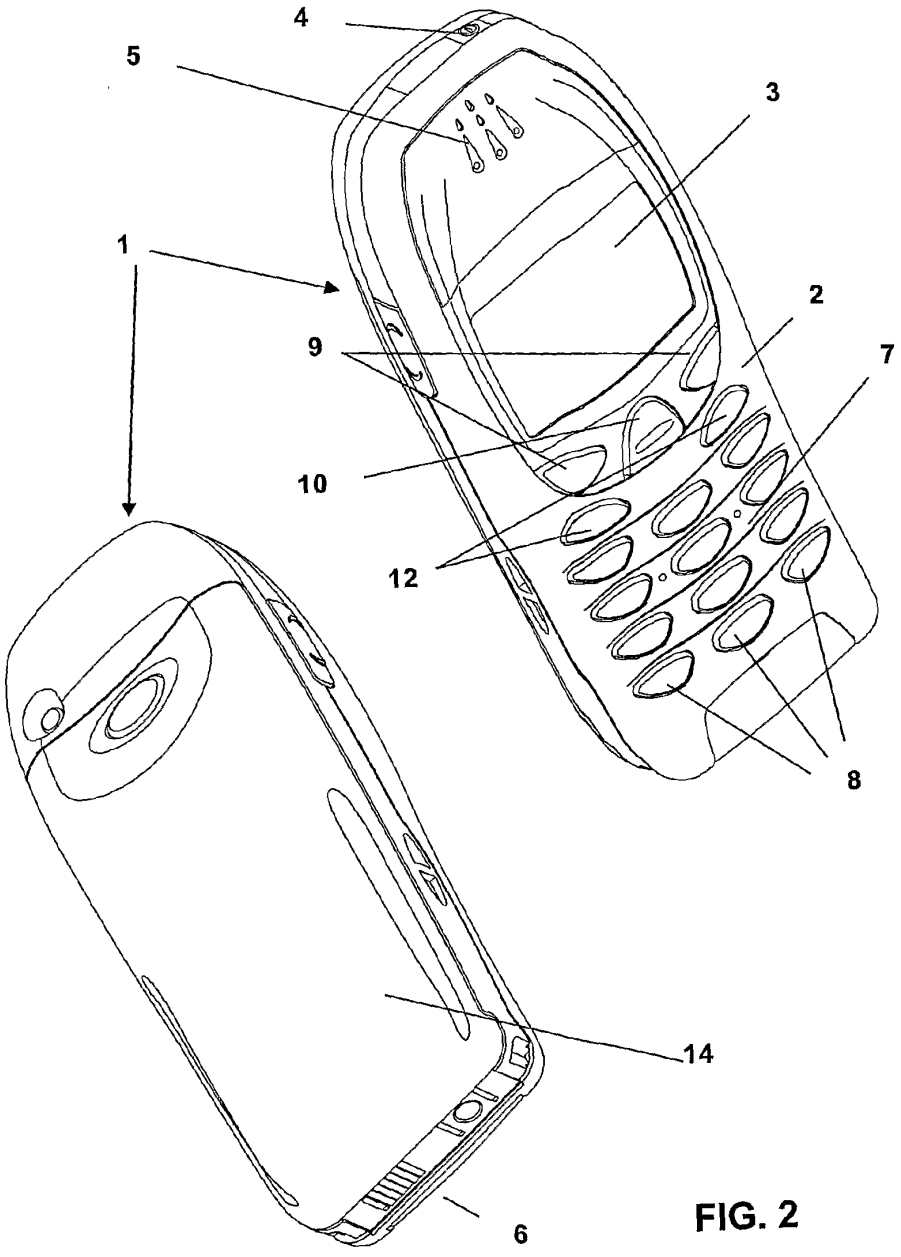


FIG. 2

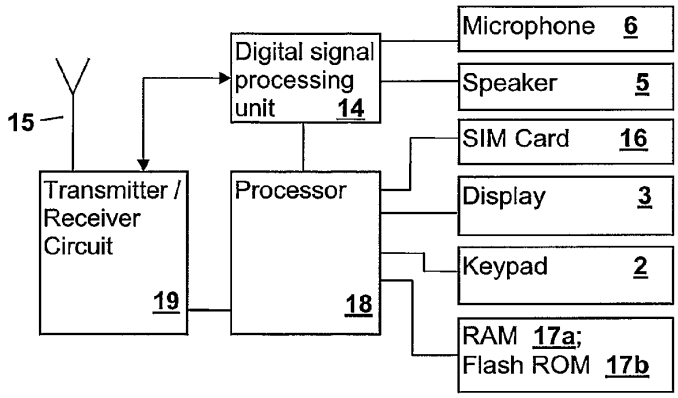

15
Digital signal processing unit 14
Microphone 6
Speaker 5
SIM Card 16
Display 3
Keypad 2
RAM 17a; Flash ROM 17b
Transmitter / Receiver Circuit 19
Processor 18

FIG. 3

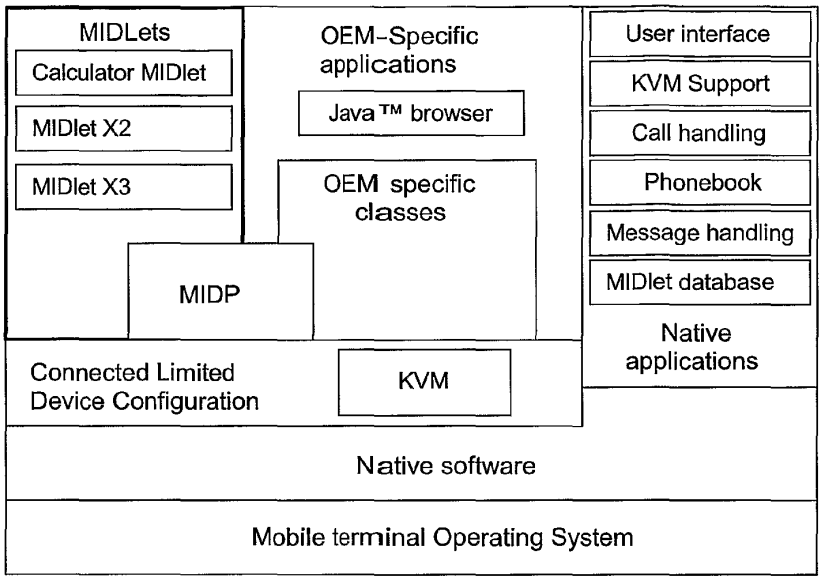

MIDLets
Calculator MIDlet
MIDlet X2
MIDlet X3
OEM-Specific applications
Java™ browser
OEM specific classes
MIDP
User interface
KVM Support
Call handling
Phonebook
Message handling
MIDlet database
Native applications
Connected Limited Device Configuration
KVM
Native software
Mobile terminal Operating System

FIG. 4

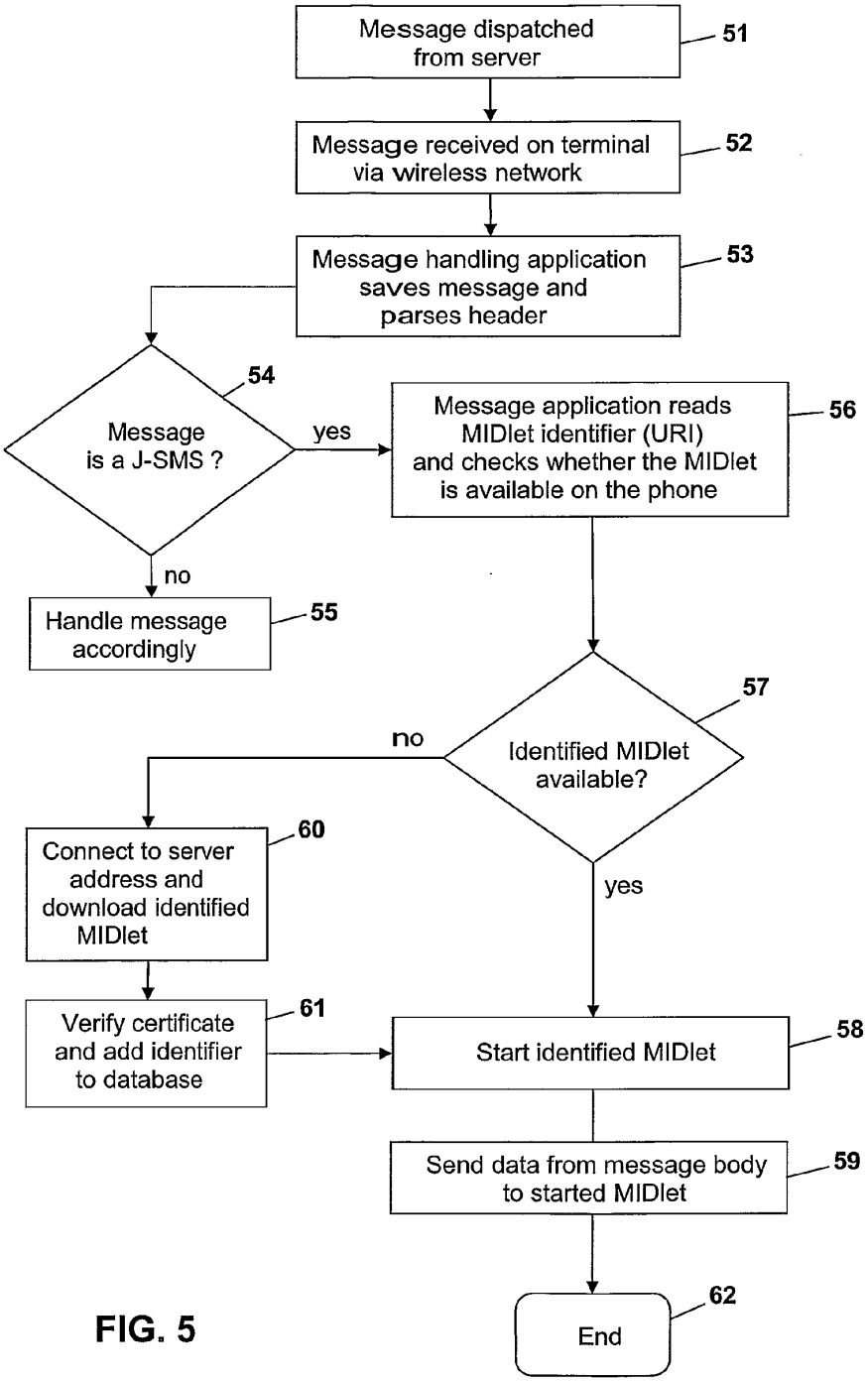

Message dispatched from server
51
Message received on terminal via wireless network
52
Message handling application saves message and parses header
53
Message is a J-SMS ?
54
yes
Message application reads MIDlet identifier (URI) and checks whether the MIDlet is available on the phone
56
no
Handle message accordingly
55
Identified MIDlet available?
57
no
yes
Connect to server address and download identified MIDlet
60
Verify certificate and add identifier to database
61
Start identified MIDlet
58
Send data from message body to started MIDlet
59
End
62

FIG. 5

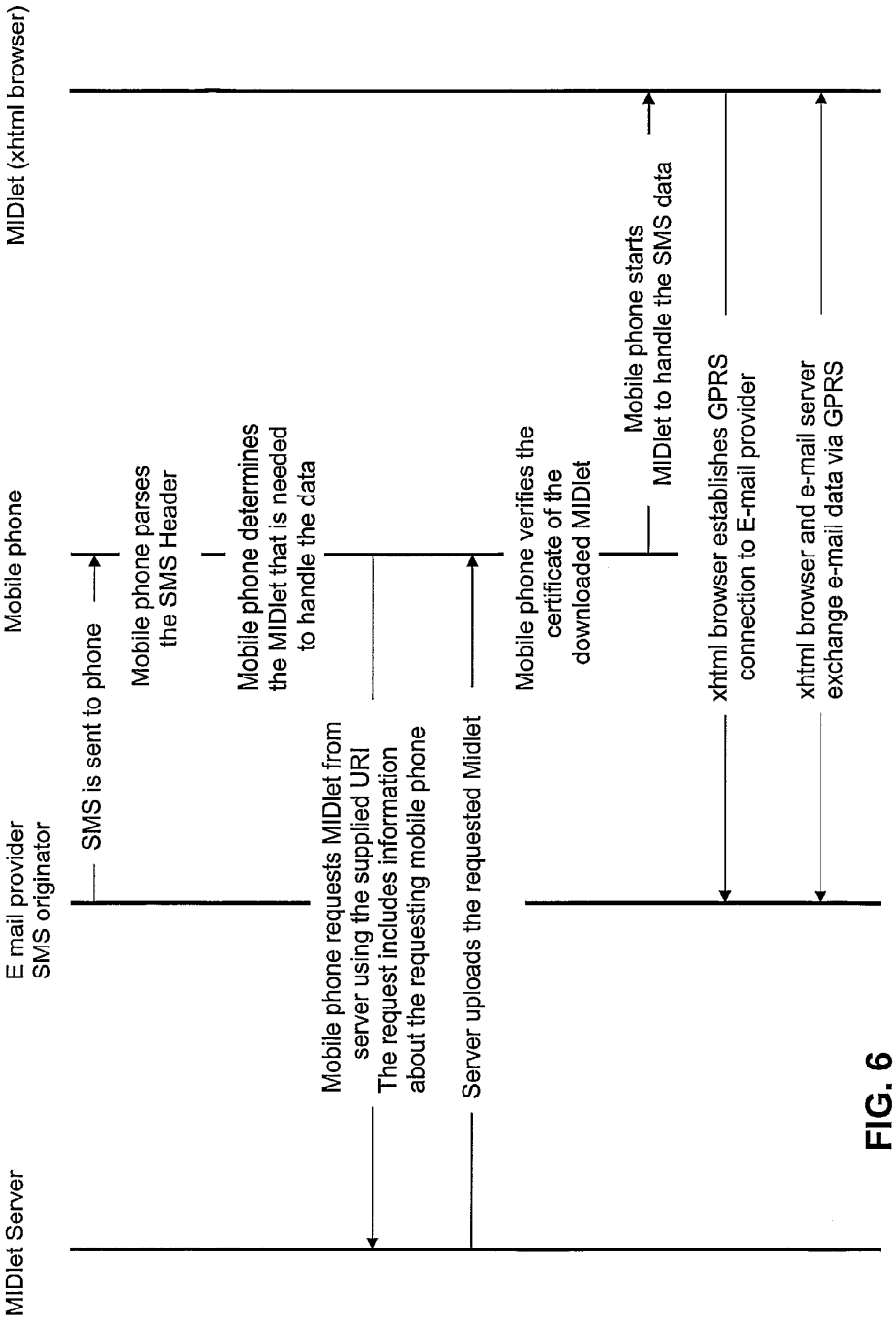

MIDlet (xhtml browser)
Mobile phone
E mail provider
SMS originator
MIDlet Server
SMS is sent to phone
Mobile phone parses the SMS Header
Mobile phone determines the MIDlet that is needed to handle the data
Mobile phone requests MIDlet from server using the supplied URI
The request includes information about the requesting mobile phone
Server uploads the requested Midlet
Mobile phone verifies the certificate of the downloaded MIDlet
Mobile phone starts MIDlet to handle the SMS data
xhtml browser establishes GPRS connection to E-mail provider
xhtml browser and e-mail server exchange e-mail data via GPRS

FIG. 6

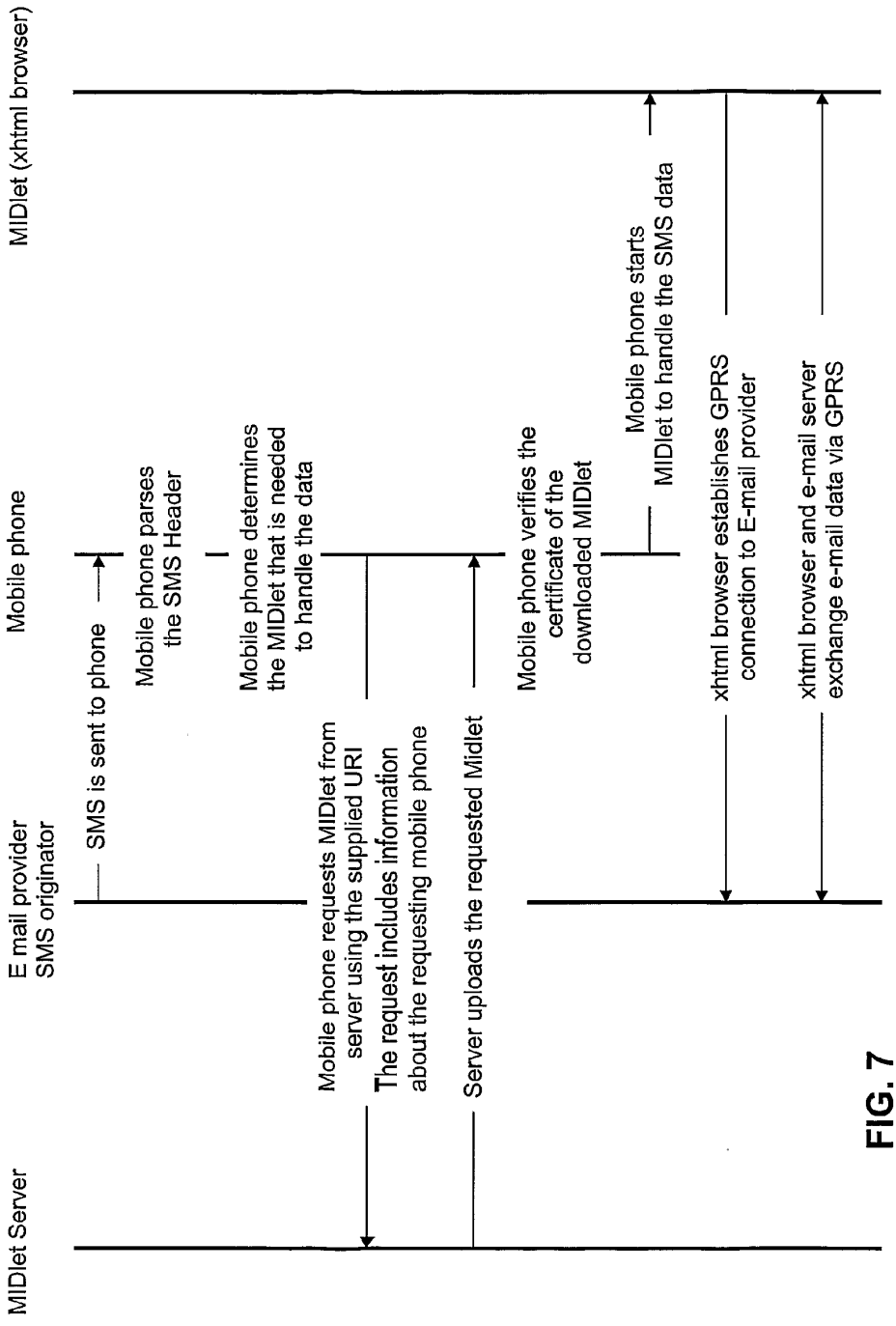

MIDlet (xhtml browser)
Mobile phone
E mail provider
SMS originator
MIDlet Server
SMS is sent to phone
Mobile phone parses the SMS Header
Mobile phone determines the MIDlet that is needed to handle the data
Mobile phone requests MIDlet from server using the supplied URI
The request includes information about the requesting mobile phone
Server uploads the requested Midlet
Mobile phone verifies the certificate of the downloaded MIDlet
Mobile phone starts MIDlet to handle the SMS data
xhtml browser establishes GPRS connection to E-mail provider
xhtml browser and e-mail server exchange e-mail data via GPRS

FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/013101

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32

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 7 H04Q

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

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

EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 98/34422 A (NOKIA MOBILE PHONES LIMITED; WELLS, MARK; HUBER, ROLF) 6 August 1998 (1998-08-06) page 5, line 4 - line 17 page 15, line 5 - page 17, line 2 page 27, line 7 - last line figure 4 ----- -/--	1,3,5,7, 9,11-15, 17-23, 26-30, 32,33

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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
11 March 2005	30/03/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Müller, N

2

Form PCT/ISA/210 (second sheet) (January 2004)

IPR2025-01572
Apple EX1002 Page 513

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/013101

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SONERA MEDIALAB: "Mobile Java Application Development White Paper" 'Online! 12 September 2002 (2002-09-12), , XP002320888 Retrieved from the Internet: URL:http://www.medialab.sonera.fi/workspace/MobileJavaAppDevelopment.pdf> 'retrieved on 2005-03-10! Chapters 1 and 2	1,3,5,7, 9,11-15, 17-23, 26-30, 32,33
A	EP 1 143 688 A (CLIENT ELECTRONICS GMBH) 10 October 2001 (2001-10-10) page 2, paragraph 10 - page 3, paragraph 20 page 3, paragraph 25 - page 5, paragraph 44 figures 1-3,5	1-45
A	US 2002/123335 A1 (LUNA MICHAEL E.S ET AL) 5 September 2002 (2002-09-05) page 1, paragraph 13 - paragraph 14 page 2, paragraph 16 page 2, paragraph 21 - paragraph 23 page 3, paragraph 27 figure 2	1-45
A	US 2002/138545 A1 (ANDREAKIS DEAN W ET AL) 26 September 2002 (2002-09-26) page 1 - page 2, paragraph 10 page 2 - page 3, paragraph 19 page 3, paragraph 22 - paragraph 24	1-45

2

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

IPR2025-01572
Apple EX1002 Page 514

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/013101

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9834422 A	06-08-1998	US 6125281 A	26-09-2000
		AU 6214998 A	25-08-1998
		WO 9834422 A2	06-08-1998
		EP 0956719 A2	17-11-1999
		JP 2001509981 T	24-07-2001
		US 6078820 A	20-06-2000
EP 1143688 A	10-10-2001	EP 1143688 A1	10-10-2001
US 2002123335 A1	05-09-2002	US 2002068554 A1	06-06-2002
		US 2003023849 A1	30-01-2003
		EP 1308858 A2	07-05-2003
		CN 1270452 A	18-10-2000
		EP 1043906 A2	11-10-2000
		JP 2000358282 A	26-12-2000
		EP 1286514 A2	26-02-2003
US 2002138545 A1	26-09-2002	CN 1460213 A	03-12-2003
		EP 1374082 A1	02-01-2004
		JP 2004519780 T	02-07-2004
		MX PA02011541 A	06-06-2003
		WO 02077843 A1	03-10-2002

IPR2025-01572
Apple EX1002 Page 515

Electronic Acknowledgement Receipt	
EFS ID:	29176369
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	10-MAY-2017
Filing Date:	06-OCT-2016
Time Stamp:	18:10:18
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)	P041D1C1.pdf	1053955 e210e43ab453905525b6f97e8e9d1fbc88071319	no	4

Warnings:

Information:					
2	Foreign Reference	2093.pdf	3514622 c65fb898082d5782c1d6c4ab30f0d6f6ceb5ae6b	no	45
Warnings:					
Information:					
			Total Files Size (in bytes):	4568577	

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	Rudy, Andrew J.
Serial No.:	15/287,597	Art Unit:	3687
Filed:	October 6, 2017	Conf. No.:	4727
Title:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems		

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

PRELIMINARY AMENDMENT

Prior to examination, please enter the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 6.

IPR2025-01572
Apple EX1002 Page 518

AMENDMENTS TO THE CLAIMS

1. (Canceled).

2. (New) A method of operating a network system, the method comprising:

receiving a first request from any first device in a plurality of similar wireless end-user devices, the first request for a secure device credential,

performing a verification step of one or more device identifiers supplied by the first device, and,

upon a successful verification in the verification step,

generating a secure device credential for the first device,

associating the secure device credential with one or more device identifiers of the first device, and

securely sending the secure device credential to the wireless end-user device;

based at least in part on the secure device credential, negotiating a secure message link between a message link server in the network system and a device link agent in the first device;

receiving, over the secure message link, a second request from the first device, the second request for a secured application credential, for any first application identified from a plurality of device applications registered to use wireless network communications, the second request comprising a general application credential for the first application; and

in response to the second request,

generating, based on the identified first application and the secure device credential, a first secured application credential unique to the first device, and

sending the first secured application credential to the first device over the secure message link.

3. (New) The method of claim 2, further comprising, in response to receiving the first request and prior to performing the verification step, returning to the first device a network system credential that is verifiable through a trusted certificate authority.

IPR2025-01572
Apple EX1002 Page 519

4. (New) The method of claim 2, wherein generating a secure device credential for the first device comprises encrypting the credential with a key known by at least one element of the network system.

5. (New) The method of claim 2, further comprising routing a network message to the identified first application over the secure message link, using the first secured application credential to indicate that the identified first application is to receive the network message.

6. (New) The method of claim 2, wherein the first secured application credential is a run-time application credential.

7. (New) The method of claim 6, further comprising receiving, from the device link agent over the secure message link, the run-time application credential, and evaluating the run-time application credential at an element of the network system.

8. (New) The method of claim 7, further comprising, in response to evaluating the run-time application credential, returning a network policy setting over the secure message link to the device link agent, the network policy setting applicable to the first application.

9. (New) The method of claim 7, wherein the element of the network system is an authentication server, the network system further comprising an application credential database coupled to the authentication server and storing secured application credentials, including the first secured application credential.

10. (New) The method of claim 2, further comprising based on a first device event, refreshing the first secured application credential to create a different secured application credential unique to the first device, and sending the different secured application credential to the first device, the different credential superseding the first secured application credential.

IPR2025-01572
Apple EX1002 Page 520

11. (New) The method of claim 2, further comprising, in response to the second request, verifying that the general application credential matches a known-application credential for the first application.

12. (New) The method of claim 11, wherein the known-application credential is uploaded to the network system via an application developer service design center.

13. (New) The method of claim 11, further comprising obtaining the known-application credential from an app store.

14. (New) The method of claim 2, the verification step further comprising evaluating a subscriber identifier associated with one or more wireless end-user devices, including the first device.

15. (New) The method of claim 14, further comprising generating the secure device credential based at least in part on one or more of the device identifiers and also on the subscriber identifier.

16. (New) The method of claim 2, further comprising forwarding network messages to the first application on the first device over the secure message link, based on the first secured application credential.

17. (New) The method of claim 2, wherein the secure device credential is a credential associated with a service processor on the first device, the method further comprising confirming the identity of the service processor based at least in part on the secure device credential.

18. (New) The method of claim 2, wherein a first subscriber is associated with both the first device and with a second wireless end-user device, the method further comprising the network system generating, based on the identified first application and a second secure device credential associated with the second device, a second secured application credential unique to the second device.

IPR2025-01572
Apple EX1002 Page 521

19. (New) The method of claim 2, wherein generating the first secured application credential comprises creating a combination of the general application credential and the secure device credential.

20. (New) The method of claim 19, wherein the combination comprises a hash.

IPR2025-01572
Apple EX1002 Page 522

REMARKS

Claim 1 has been canceled, and new claims 2-20 have been added. No new matter has been added. Applicant respectfully requests the entry of the amendments herein.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: June 9, 2017

By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(512) 970-9135

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: June 9, 2017 By: /Ann Taylor/
Ann Taylor

IPR2025-01572
Apple EX1002 Page 523

Electronic Acknowledgement Receipt	
EFS ID:	29453450
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	09-JUN-2017
Filing Date:	06-OCT-2016
Time Stamp:	16:31:46
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		P041C1D1_PA.pdf	76222 9a78ca47e5390550ef73e1ad7662db5a1d4460e4	yes	6

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	6
Warnings:			
Information:			
	Total Files Size (in bytes):	76222	

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.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/287,597	Filing Date 10/06/2016	☐ 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), (i), 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(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ 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

AMENDMENT		(Column 1)		(Column 2)	(Column 3)		
	06/09/2017	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 19	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $210 =	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		(Column 1)		(Column 2)	(Column 3)		
		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 number found in the appropriate box in column 1.

LIE
LINDA HUMES

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1

CONFIRMATION NO. 4727

106963
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

PUBLICATION NOTICE

OC000000092445077

Title: Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

Publication No.US-2017-0188232-A1
Publication Date:06/29/2017

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 Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IPR2025-01572
Apple EX1002 Page 527

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP041D1C1

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	6466984	B1	2002-10-15	Naveh et al.	
	2	6522629	B1	2003-02-18	Anderson, Sr., Ronald D.	
	3	6996062	B1	2006-02-07	Freed et al.	
	4	7269157	B2	2007-09-11	Klinker et al.	
	5	7340772	B2	2008-03-04	Panasyuk et al.	
	6	7423971	B1	2008-09-09	Mohaban et al.	
	7	7522576	B2	2009-04-21	Du et al.	
	8	7769397	B2	2010-08-03	Funato et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	9	7882247	B2	2011-02-01	Sturniolo et al.	
	10	7925740	B2	2011-04-12	Nath et al.	
	11	8010990	B2	2011-08-30	Ferguson et al.	
	12	8159520	B1	2012-04-17	Dhanoa et al.	
	13	8446831	B2	2013-05-21	Kwan et al.	
	14	8499087	B2	2013-07-30	Hu, Qingmin	
	15	8619735	B2	2013-12-31	Montemurro et al.	
	16	8826411	B2	2014-09-02	Moen et al.	
	17	9015331	B2	2015-04-21	Lai et al.	
	18	9402254	B2	2016-07-26	Kneckt et al.	
	19	9634850	B2	2017-04-25	Taft et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

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	20050111463	A1	2005-05-26	Leung et al.	
	2	20090149154	A1	2009-06-11	Bhasin et al.	
	3	20090291665	A1	2009-11-26	Gaskarth et al.	
	4	20110177811	A1	2011-07-21	Heckman et al.	

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	0208863	WO		2002-01-31	Telemac Corp.		

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		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

If you wish to add additional non-patent literature document citation information please click the Add button	Add		
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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

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	/James E. Harris/	Date (YYYY-MM-DD)	2017-08-11
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

IPR2025-01572
Apple EX1002 Page 533

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/08863 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/23226

(22) International Filing Date: 23 July 2001 (23.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/220,241 21 July 2000 (21.07.2000) US

(71) Applicant: **TELEMAC CORPORATION** [US/US]; 6701 Center Drive West, Suite 700, Los Angeles, CA 90045 (US).

(72) Inventors: **WATLER, Theodore, W.**; 5341 E. 4th Street, Long Beach, CA 90814-1920 (US). **HANLEY, Jerry**; 1315 Franklin Street, #D, Santa Monica, CA 90404 (US).

(74) Agents: **NG, Horace** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834 (US).

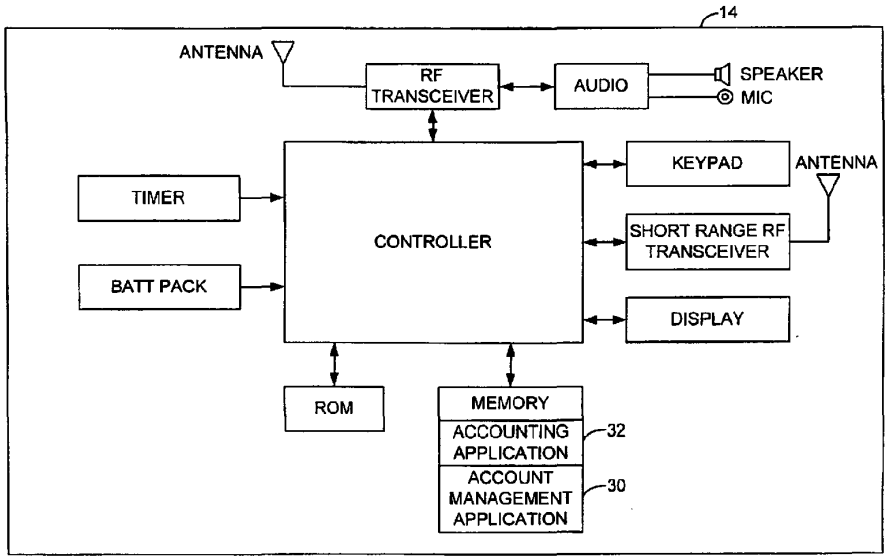
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: MULTIPLE VIRTUAL WALLETS IN WIRELESS DEVICES



(57) Abstract: A system having a wireless device capable of monitoring and tracking its own usage and account activities is disclosed. The wireless device includes an account management application and accounting applications. The account management application manages a variety of accounts in conjunction with the accounting applications and is used by a user to determine how each call/transaction is to be paid for. For example, the user of the wireless device may wish to pay for business calls using a first account and personal calls using a second account.

WO 02/08863 A2

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.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 535

MULTIPLE VIRTUAL WALLETS IN WIRELESS DEVICES

CROSS-REFERENCES TO RELATED APPLICATION

[01] This application claims the benefit of priority under 35 U.S.C. § 119 from U.S. Provisional Patent Application Serial No. 60/220,241 filed on July 21, 2000, the disclosure of which is hereby incorporated by reference in its entirety for all purposes.

BACKGROUND OF THE INVENTION

[02] The present invention generally relates to a system with an account management protocol for wireless devices, and in particular, to a system with an account management protocol which is used to monitor and track usage and account activities of a wireless device.

[03] More specifically, the account management system is adapted for a mobile phone so as to allow the usage and account activities of the mobile phone to be tracked and monitored on an individual basis. A number of accounting systems are described in U.S. Patent Nos. 5,325,418 (the '418 Patent), 5,625,669 (the '669 Patent), 5,577,100 (the '100 Patent), and 6198,915 B1 (the '915 Patent), which are incorporated herein by reference. The '418 and '669 Patents describe accounting systems with features that have particular application to post-paid mobile phone services, such as a mobile phone rental service or controlled mobile phone services. In a controlled mobile phone service, capturing phone call data and calculating phone charges for each call enable service providers (or corporations in an intra-corporate system) to limit, or at least monitor, mobile phone usage before the periodic billing cycle. For example, if mobile phone usage exceeds a pre-established limit, the mobile phone could be temporarily disabled or restricted until an interim payment or additional credit sources are obtained. In an intra-corporate system, a warning message could be sent to a corporate authority that could then either authorize additional use or temporarily disable the mobile phone. In such systems, phone call data is stored in the mobile phone and then transmitted to a host processor that calculates charges. The host processor is typically located on a network that is separate from the mobile phone.

[04] Since the issuance of the '418 and '669 Patents, the state of the art has advanced to a point where an accounting application in the mobile phone is able to calculate calling charges internally. As described in the '100 and '915 Patents, such

IPR2025-01572
Apple EX1002 Page 536

systems minimize the communication traffic required between the service provider's host processor and the mobile phone and thus expand the overall traffic handling capacity of the mobile phone system. The '100 and '915 Patents describe accounting systems with features that have particular application to pre-paid mobile phone services.

[05] Due to the increasing ease of use and lower costs, the proliferation and use of mobile phones is going to continue. Many companies nowadays provide employees with mobile phones in order to ensure that such employees remain in contact. Since carrying two mobile phones is quite impractical, these employees inevitably tend to use their company-provided mobile phones for both business and personal calls. Hence, in order to prevent abuses and/or provide accurate accounting, it would be desirable to have the ability to monitor proper usage and account activities of company-provided mobile phones.

[06] Furthermore, some mobile phones on the market today provide a two-line or multi-line capability. With a two-line phone, the two phone lines could be dedicated to handle a first type and a second type of calls respectively. As a result, account activities for different types of calls may need to be monitored separately. Therefore, it would be desirable to provide a mobile phone system that is capable of handling and monitoring different types of usage and account activities for wireless devices.

SUMMARY OF THE INVENTION

[07] The system of the present invention relates to wireless communication systems having wireless devices, particularly mobile phones, that are part of a wireless communication network. In particular, the present invention relates to a wireless device, such as a mobile phone, that includes an internal account management application for internal management of a variety of accounts. In an exemplary embodiment, the account management application interacts with an accounting application for calculation of communication charges on the fly. Such mobile phones are typically cellular telephones in a cellular phone network, radio telephones in a personal communication service network or other communication system, where the mobile phone is moveable from place to place.

[08] Use of the system of the present invention is intended for mobile phones, where real time calculation of calling charges is desirable to limit phone usage or to immediately bill for phone usage where the billings of the public switched service providers and participating wireless service providers are not yet available.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 537

[09] The account management system includes an account management application, carried internally in the wireless device, that manages a variety of accounts. The account management application interacts with one or more accounting applications, such as, a complex billing algorithm with multiple factor accounting protocol to account for local charges, roaming charges when the wireless device moves from one zone to another, long distance charges, international charges including country independent local charges, and surcharges which may be per call or rate based. The complex billing algorithm can be expanded to accommodate special charges of service providers or called stations or special discounts or premiums for data transfer calls.

[10] The accounting applications related to mobile phone usage may include a rate schedule. A rate schedule in the wireless device may be periodically updated by wireless communications with the service provider's host processor or customer service representative. The accounting applications related to m-commerce transactions obtain the amount to be deducted from a pre-defined communication protocol with the vendor's transaction device or customer service representative.

[11] It is to be understood that the accounting applications may reside either in the wireless device or on a network which is accessible to the wireless device. Depending on design specification or constraints, the functionality of the account management application may be incorporate into the accounting application.

[12] It is to be further understood that the wireless device with the account management system can be implemented into existing wireless communication networks without substantial modification to the network and can be implemented into most existing wireless devices with minimal modification, primarily by internal reprogramming of the wireless device. Modification to most existing wireless devices is even more minimal when existing accounting applications residing on a network are utilized by the wireless device.

[13] A wireless device such as a mobile phone currently includes an internal processor and sufficient internal memory to incorporate the programming and data storage necessary to accomplish the real time accounting. The account management application and the complex algorithms providing the multiple factor accounting capabilities are sufficiently compact that storage and processing of the call data is enabled in real time with sufficient accuracy to account for multiple charges from multiple service providers even for a roaming phone. The accounting and account management

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 538

applications should utilize an encryption system to permit secure programming and transactions over the airways.

[14] The accounting and account management system as described herein provides customers and businesses with greater flexibility in managing costs of mobile phone use and m-commerce transactions, especially where costs must be segregated into different accounts by multiple criteria such as business versus personal, or by different profit centers within the same business. The increased flexibility also includes different methods for controlling costs with respect to each account such as pre-paid service or post-paid service with usage limits. The present invention describes a system in which an individual wireless device could be utilized in a controlled service mode for certain purposes such as business calls, in a pre-paid service mode for other purposes such as private calls, and have additional secure electronic accounts for other m-commerce transactions.

[15] The system of the present invention is adapted for analog or digital cellular telephones, radiophones in personal communication service networks and other wireless communication systems. The system is also adapted for other wireless devices, such as personal digital assistants, that are used for m-commerce transactions through short-range radio frequency communication protocols or data bearer communication services such as short message service.

[16] Reference to the remaining portions of the specification, including the drawings and claims, will realize other features and advantages of the present invention. Further features and advantages of the present invention, as well as the structure and operation of various embodiments of the present invention, are described in detail below with respect to accompanying drawings, like reference numbers indicate identical or functionally similar elements.

BRIEF DESCRIPTION OF THE DRAWINGS

[17] Fig. 1 is a simplified schematic diagram illustrating a typical wireless telecommunication arrangement;

[18] Fig. 2 is a simplified schematic diagram illustrating a typical arrangement for sending data bearer messages such as short message service to a wireless device;

[19] Fig. 3 is a simplified schematic diagram illustrating a typical wireless transaction arrangement; and

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 539

[20] Fig. 4 is a simplified schematic diagram showing an exemplary embodiment of a wireless device in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[21] Fig. 1 is a simplified schematic diagram illustrating a typical wireless telecommunication arrangement. A network 10 communicates with a wireless device 14, such as a mobile phone, via a transmission station 12. The transmission station 12 uses over-the-air communications to communicate with the wireless device 14. Over-the-air communication protocols which can be used to implement wireless communications between the wireless device 14 and the network 10 include, for example, GSM, CDMA, TDMA, UMTS, etc. A person of ordinary skill in the art will know of other ways and methods to implement over-the-air communications.

[22] Fig. 2 is a simplified schematic diagram illustrating a typical arrangement for sending data bearer messages such as short message service to a wireless device 14. An application program 16 residing on a host processor 18 uses a communication link 20, such as a TCP/IP link over the Internet, to communicate with a data bearer message controller 22 within the network 10 to transmit a data bearer message such as a short message service message to the wireless device 14, such as a mobile phone, via a transmission station 12.

[01] Fig. 3 is a simplified schematic diagram illustrating a typical wireless transaction arrangement. A vending machine 24 with a short range radio communication transceiver and the wireless device 14, such as a mobile phone with a short range radio communication transceiver, communicate using a short range radio communication link 26. Short range radio communication links which can be used to implement wireless communications between the wireless device 14 and the vending machine 24 include, for example, Bluetooth ™ wireless communication links. A person of ordinary skill in the art will know of other ways and methods to communicate transactional data between two devices. As another example, vending machine 24 and wireless device 14, each with the appropriate transceiver, can communicate transactional data using a data bearer message service such as short message service.

[24] Referring to Fig. 4, there is shown an exemplary embodiment of the wireless device 14 in accordance with the present invention. According to the exemplary embodiment, the wireless device 14 includes an account management application 30 which permits the usage and account activities of the wireless device 14 to be tracked and

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 540

monitored on an individual basis. The account management application 30 functions as multiple virtual wallets and is capable of maintaining a number of different accounts which are chargeable for calls or transactions handled by the wireless device 14. The different accounts include, for example, traditional postpaid account, postpaid monitored or controlled usage account, and prepaid account.

[25] The account management application 30 can reside on executable memory within the wireless device 14. Such memory can be one of any type such as ROM, EPROM, or flash memory. The account management application 30 can store dynamic data in RAM and utilize nonvolatile memory such as EEPROM or flash memory to store control data. Alternatively, the account management application 30 can reside on a smart card, such as a universal subscriber identification module (USIM) or Universal Identity Module (UIM), which is attachable to the wireless device 14.

[26] According to an exemplary embodiment, the account management application 30 further interacts with other applications, such as the accounting application 32 described below, so as to properly manage and process the different accounts. The accounting application 32 is capable of calculating calling charges in real time or on the fly. An example of the accounting application 32 is the complex billing algorithm described in the '100 Patent. The complex billing algorithm factors the multiple variables of a telephone call from a mobile phone into a billing equation that virtually mirrors the factors considered by public switched network providers and participating wireless service providers, (of which there may be more than one in a single call). The resultant call charge accurately approximates the summation of real charges that will be billed by the participating service providers thereby enabling an instantaneous calculation and display of calling charges. The complex billing algorithm can be expanded to accommodate special charges of service providers or called stations or special discounts or premiums for data transfer calls. The accounting application 32 can reside on executable memory within the wireless device 14. Such memory can be one of any type such as ROM, EPROM, or flash memory. The accounting application 32 can store dynamic data in RAM and utilize nonvolatile memory such as EEPROM or flash memory to store control data. Alternatively, the accounting application 32 can reside on a smart card, such as a universal subscriber identification module (USIM) or Universal Identity Module (UIM), which is attachable to the wireless device 14. In the alternative, it is to be also understood that the accounting application 32 may reside on the network 10. A

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 541

person of ordinary skill in the art will know of ways and methods to obtain and retrieve calling charge information from an accounting application 32 residing on the network 10.

[27] It is to be further understood that the accounting applications 32 may reside either in the wireless device 14 or on the network 10 which is accessible to the wireless device 14. Depending on design specification or constraints, the functionality of the account management application 30 may be incorporated into or combined with the accounting application 32.

[28] The wireless device 14 can be programmed using systems such as that described in U.S. Patent No. 6,243,574 B1. In addition to installing account management application 30 and accounting applications 32, programming can include providing data, such as initial monetary values for pre-paid accounts or credit limits, to the wireless device 14. Alternatively, the wireless device 14 can be programmed over the air using DTMF signals, or a data bearer communication service such as short message service, initiated from an application program 16 residing on a host processor 18 such as described in the '100 Patent.

[29] The wireless device 14 is preferably a contemporary unit with an LCD display screen for display of numeric or alphanumeric data, such as a user menu and warning messages; a keypad for entry of data, such as menu selections; and a timer for determining the duration of calls thereby allowing calling charges to be calculated. In the alternative, a person of ordinary skill in the art will know that timer information can be obtained from the network 10.

[30] In an exemplary embodiment, the account management application 30 charges a call or transaction to the account selected by a user. The account selection is accomplished via a user interface. The user interface permits the user to interact with the account management application 30 and select which one of the accounts is to be used for each call or transaction. Furthermore, the user interface also allows the user to perform certain account management functions. For example, the user, via the user interface, may transfer balances between accounts or perform other typical accounting functions. As another example, the user, via the user interface, may change the account to which a particular call has been charged. Preferably, the user interface is implemented in the form of a menu of available accounts presented on the LCD screen of the wireless device 14.

[31] In an exemplary mode of operation, the usage and account activities of the wireless device 14 are monitored and tracked as follows. In the situation where an outgoing call is to be made via the wireless device 14, before such call is made, the user

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 542

using the user interface selects which account is to be charged for that call. Once the account is selected, the user then continues with the normal procedures to make the call. If, for example, a prepaid account is selected, the accounting application 32 then calculates the charges to be debited and the account management application 30 accordingly debits the selected prepaid account.

[32] Similarly, in the situation where an incoming call is to be received by the wireless device 14, before such call is answered, the user using the user interface selects which account is to be charged for that call. Once the account is selected, the user then continues with the normal procedures to receive the call. If, for example, a postpaid account is selected, the charges for the call are calculated and the account management application 30 accordingly updates the postpaid account.

[33] As described above, a selected account is charged for a call handled by the wireless device 14. However, it should be understood that an account may also be charged for any transaction handled by the wireless device 14. That is, the account management application 30 is also able to monitor and track transactions handled by the wireless device 14. For example, referring to Fig. 3, if the wireless device 14 is used to communicate with the vending machine 24 to make a purchase, an appropriate account on the wireless device 14 can similarly be charged for making that purchase.

[34] Alternatively, the account management application 30 may automatically select the account to be charged from a multifactor algorithm. For example, where the wireless device 14 is a multi-line mobile phone, the account management application 30 detects which line of the multi-line mobile phone is in use and charges the account associated with that line. The calling charges to be applied to that account is determined by the accounting application 32. For example, the account management application 30 may select and apply a postpaid account for calls made or received on one line and select and apply a prepaid account for calls made or received on another line.

[35] In another exemplary embodiment, the account management application 30 is able to determine the telephone number of the device which originated the call using the network 10 automatic number identification features, and charge the account associated with that telephone number in a table stored on EEPROM or flash memory within the wireless device 14. In the event that the originating telephone number was not found in the table, a default account is then charged or the user is prompted to select an account to be charged for the call. The timing of the prompt may vary depending on design. For example, the prompt may occur after the call is concluded, if the available

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 543

prepaid fund and/or credit limit of all potentially chargeable accounts was sufficient. Alternatively, the timing of the prompt may also occur at the preprogrammed time for warning of exhaustion of the available prepaid fund and/or credit limit based on the account, out of all potentially chargeable accounts, which first reaches the time for such warning. It is understood that the multifactor algorithm may include one or more of the above factors, as well as other factors appropriate for selecting the account to be charged.

[36] In an exemplary embodiment , the account management application 30 maintains each account according to an algorithm programmed by the service provider or by authorized corporate personnel. For example, an application program 16 residing on a host processor 18 can provide secure access to authorized corporate personnel to allow such personnel to enter control data with respect to each account. The application program 16 can initiate the transmission of a data bearer message, such as a short message service message, which, when received by the wireless device 14, accordingly reprograms the wireless device 14 with such control data. For example, one account may be set up to be a traditional postpaid account with a limit on usage and a second account may be set up to be a prepaid account. Corporate procedures may require the user to use the first account only for legitimate business calls. The user's compliance with such procedures may be monitored through call detail records stored on the wireless device 14 and transmitted to a host processor as described in the '418 and '669 Patents.

[37] It is understood that the call detail records can be stored on RAM or other memory within the wireless device 14, or alternatively, the call detail records can be stored on a smart card, such as a universal subscriber identification module (USIM), which is attachable to the wireless device 14.

[38] The control data transmitted to the wireless device 14 can also be used to determine the consequence of the user reaching a usage limit. For example, one such consequence is for the account management application 30 to generate and transmit an SMS message, or other data bearer message, to the appropriate corporate authority warning that the user had exceeded the usage limit and that review of the call detail records is warranted. Another such consequence is for the account management application 30 to temporarily restrict operation of the wireless device 14, allowing only emergency calls and calls to customer representatives until the restriction is removed. Corporate procedures may permit personal calls on the same wireless device 14 if the user utilizes the second account, the prepaid account. Authorized corporate personnel may receive acceptable forms of payment from the user, and, using the application program

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 544

16, transmit control data to the wireless device 14 adding funds to the prepaid account accordingly, similar to the description in the '100 Patent.

[39] In another exemplary embodiment, an application program 16 on a host processor 18 is able to provide secure access to authorized personnel of a service provider or, in an intra-corporate system, of the corporation to change control data with respect to each account. The application program 16 can initiate the transmission of a data bearer message, such as a short message service message, which, when received by the wireless device 14, accordingly reprograms the wireless device 14 with such control data. Examples of such changes include changes in the rate tables utilized by the accounting application 32, changes in credit limits for controlled post-paid accounts, and changes in paid funds in pre-paid accounts etc. Alternatively, the users may be provided with over the air access to application program 16 on the host processor 18 to make limited changes, such as using credit cards or prepaid calling cards to add funds to pre-paid accounts, similar to the description provided in the '100 Patent. Furthermore, the updated rate table may be transmitted to the wireless device 14 when the user applies for an increase in the internal phone account.

[40] In an exemplary embodiment, the account management application 30 is able to generate audio warnings through the speaker of the wireless device 14 and/or warning messages displayed on the LCD screen of the wireless device 14 so as to inform the user that s/he is about to exhaust the credit limit or prepaid funds. The warning messages may include information identifying the applicable account and the amount of remaining funds or credit.

[41] The system of the present invention provides substantial flexibility by the features described above. For example, a user of the wireless device 14 is given the flexibility to pay for each call differently on an ad hoc basis. A user may wish to separate and pay for the calls based on the nature of each call. Business and personal calls handled by the same wireless device 14 may be paid from different accounts. A business call is to be paid from one account and a personal call is to be paid from another account. A user may also wish to use different accounts to pay for different calls; one call may be paid from a prepaid account, while another call may be charged to a postpaid account.

[42] It is understood that the examples and embodiments described herein are for illustrative purposes only and that various modifications or changes in light thereof will be suggested to persons skilled in the art and are to be included within the spirit and purview of this application and scope of the appended claims. All publications, patents,

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 545

and patent applications cited herein are hereby incorporated by reference for all purposes in their entirety.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 546

WHAT IS CLAIMED IS:

1. A system for handling a plurality of account activities, comprising:
a wireless device capable of performing a plurality of billable operations;
an account management application residing in the wireless device;
wherein the account management application is configured to manage a plurality of accounts; and
wherein each billable operation performed by the wireless device is selectively charged to one of the plurality of accounts.

2. The system according to claim 1 further comprising:
a user interface configured to allow a user to determine how each billable operation performed by the wireless device is to be selectively charged to one of the plurality of accounts.

3. The system according to claim 1 wherein the account management application automatically selects one of the plurality of accounts to be charged for at least one of the plurality of billable operations in accordance with an algorithm.

4. The system according to claim 1 further comprising:
an accounting application configured to calculate charges for each billable operation performed by the wireless device;
wherein the account management application functions in cooperation with the accounting application to manage the plurality of accounts.

5. The system according to claim 1wherein the plurality of billable operations includes making or receiving a voice or data communication.

6. The system according to claim 5 wherein how each billable operation performed by the wireless device is to be selectively charged to one of the plurality of accounts depends on origin or destination of the voice or data communication.

7. The system according to claim 1 wherein the wireless device is a mobile phone.

8. The system according to claim 1 wherein the account management application resides on a smart card attachable to the wireless device.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 547

9. The system according to claim 1 wherein the account management application resides on a memory residing in the wireless device.

10. The system according to claim 1 wherein the accounting application resides on a memory residing in the wireless device.

11. The system according to claim 1 wherein the accounting application resides on a network.

12. The system according to claim 1 wherein the account management application is configured so as to allow a user to transfer balances amongst the plurality of accounts.

13. The system according to claim 1 wherein the plurality of accounts includes a postpaid account and a prepaid account.

14. The system according to claim 1 wherein at least one of the plurality of accounts has a usage limit; and

wherein the plurality of billable operations performable by the wireless device is restricted when the usage limit is exceeded.

15. A wireless device configured to perform a plurality of billable operations, comprising:

an account management application residing on the wireless device and configured to maintain a plurality of accounts;

an accounting application configured to calculate charges for each billable operation performed by the wireless device; and

a user interface configured to allow a user to selectively determine how each billable operation performed by the wireless device is to be charged to one of the plurality of accounts;

wherein the account management application and the accounting application function in cooperation with each other in order to maintain the plurality of accounts.

16. The wireless device of claim 15 wherein the plurality of billable operations includes making or receiving a voice or data communication.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 548

17. The wireless device of claim 16 wherein how each billable operation performed by the wireless device is to be selectively charged to one of the plurality of accounts depends on origin or destination of the voice or data communication.

18. The wireless device of claim 15 wherein the wireless device is a mobile phone.

19. The wireless device of claim 15 wherein the account management application resides on a smart card attached to the wireless device.

20. The wireless device of claim 15 wherein the account management application resides on a memory residing in the wireless device.

21. The wireless device of claim 15 wherein the accounting application resides on a network.

22. The wireless device of claim 15 wherein the account management application is configured so as to allow the user to transfer balances amongst the plurality of accounts.

23. The wireless device of claim 14 wherein the plurality of accounts includes a postpaid account and a prepaid account.

24. The wireless device of claim 14 wherein at least one of the plurality of accounts has a usage limit; and

wherein the plurality of billable operations performable by the wireless device is restricted when the usage limit is exceeded.

25. A mobile phone comprising:

a first line and a second line both configured to make and receive calls; and

an account management application residing on the mobile phone and configured to manage a plurality of accounts;

wherein calls made or received via the first line is charged to one of the plurality of accounts and calls made or received via the second line is charged to another one of the plurality of accounts.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 549

26. The mobile phone of claim 25 further comprising:

a user interface configured to allow a user to selectively determine how each call made or received by the mobile phone is to be charged to one of the plurality of accounts.

27. The mobile phone of claim 25 further comprising:

an accounting application configured to calculate charges for each call made or received by the mobile phone.

28. The mobile phone of claim 25 wherein the account management application resides on a smart card attachable to the mobile phone.

29. The mobile phone of claim 25 wherein the account management application resides on a memory residing in the mobile phone.

30. The mobile phone of claim 27 wherein the accounting application resides on a memory residing in the mobile phone.

31. The mobile phone of claim 27 wherein the accounting application resides on a network.

32. The mobile phone of claim 25 wherein the plurality of accounts includes a postpaid account and a prepaid account.

33. The mobile phone of claim 25 wherein the calls made or received via the first line include business calls and the calls made or received via the second line include personal calls.

34. The mobile phone of claim 25 wherein the account management application is configured so as to allow the user to transfer balances amongst the plurality of accounts.

35. A method for tracking account activities relating to a plurality of billable operations performable by a wireless device, comprising:

selecting one of a plurality of accounts to be charged for a billable operation, wherein the plurality of accounts are maintained on the wireless device;

calculating charges to be paid for the billable operation;

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 550

causing the wireless device to perform the billable operation; and

updating the selected account.

36. The method according to claim 35 wherein the step of selecting one of the plurality of accounts further comprises:

allowing a user to select one of the plurality of accounts via a user interface.

37. The method according to claim 35 wherein the step of calculating charges to be paid for the billable operation is performed by an accounting application.

38. The method according to claim 35 wherein the accounting application resides on a memory residing in the wireless device.

39. The method according to claim 35 wherein the accounting application resides on a network.

40. The method according to claim 35 wherein the wireless device is a mobile phone.

41. The method according to claim 35 wherein the billable operation includes making or receiving a voice or data communication.

42. The method according to claim 41 wherein the step of selecting one of a plurality of accounts to be charged for the billable operation further comprises:

identifying origin or destination of the voice or data communication;

selecting the one of the plurality of accounts to be charged for the billable operation based on the identified origin or destination of the voice or data communication.

43. The method according to claim 35 further comprising:

restricting ability of the wireless device to perform the billable operation when credit limit of at least one of the plurality of accounts is exceeded.

44. The method according to claim 35 further comprising:

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 551

restricting ability of the wireless device to perform the billable operation when prepaid level of at least one of the plurality of accounts is exhausted or goes below a pre-established limit.

45. A method for tracking account activities made by a mobile phone having a first line and a second line both configured to make and receive calls, comprising:

assigning a first account to calls made or received via the first line;

assigning a second account to calls made or received via the second line, wherein the first and second accounts are maintained on the mobile phone;

making or receiving a call via either the first line or the second line;

calculating charges to be paid for the call; and

updating either the first account or the second account based on the calculated charges depending on which one of the first and second lines the call is made or received.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 552

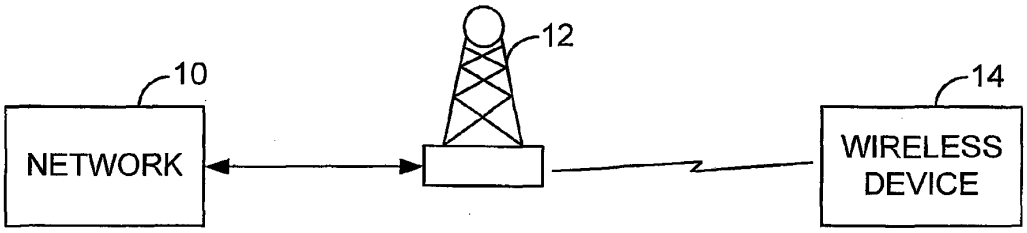


FIG. 1.

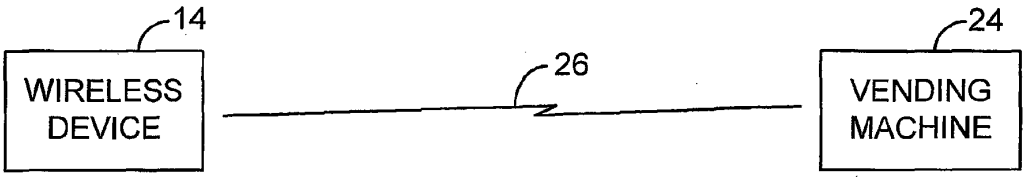


FIG. 3.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 553

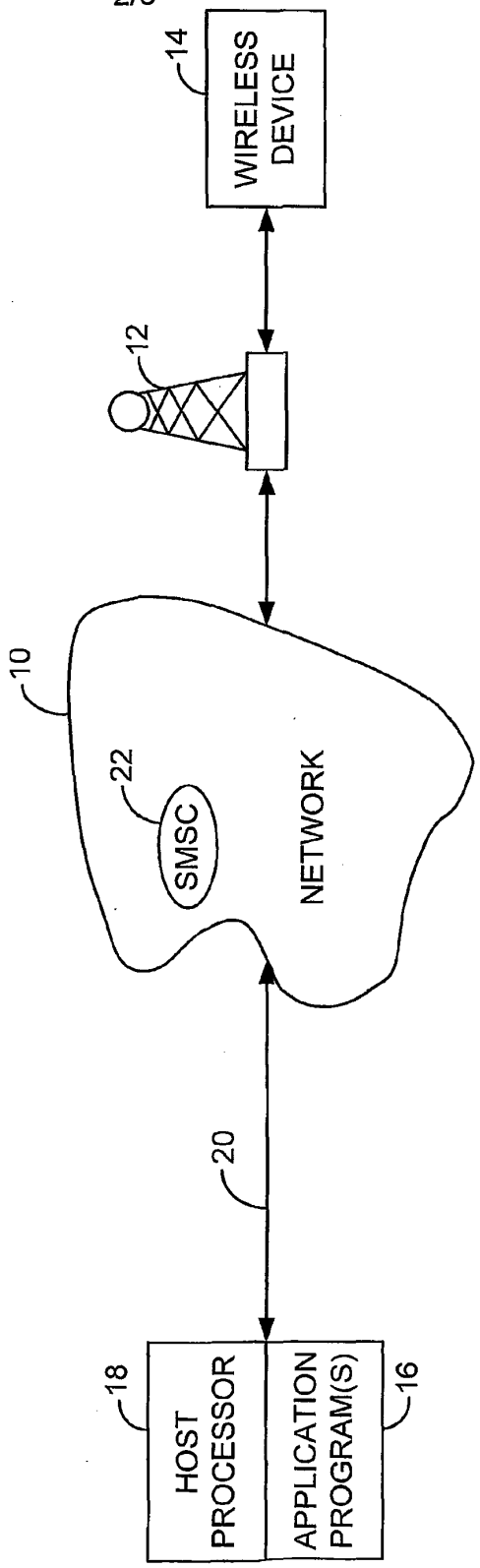


FIG. 2.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 554

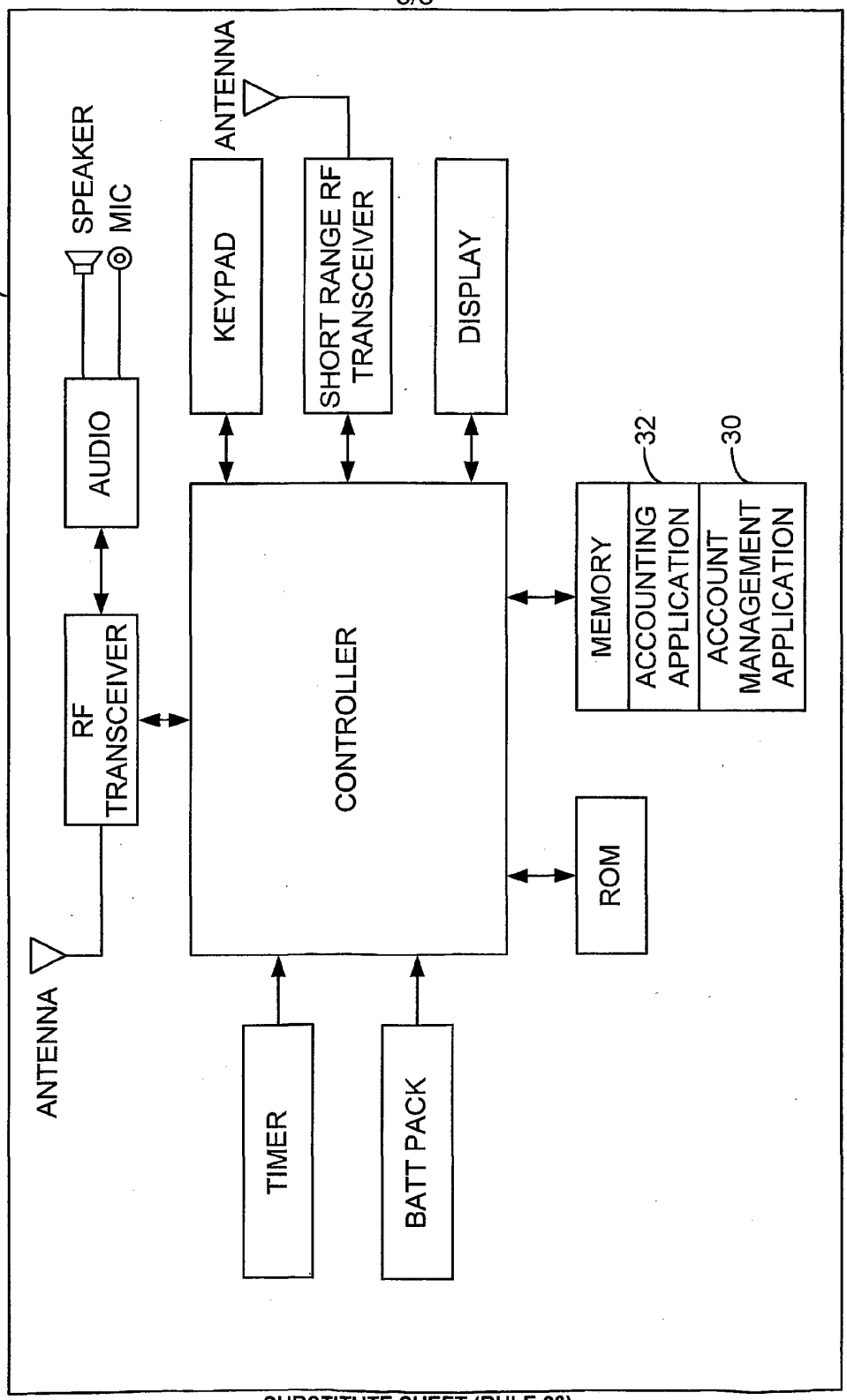


FIG. 4.

BNSDOCID: <WO_____0208863A2_I_>

IPR2025-01572
Apple EX1002 Page 555

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/08863 A3

(51) International Patent Classification[7]: H04M 15/00

(21) International Application Number: PCT/US01/23226

(22) International Filing Date: 23 July 2001 (23.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/220,241 21 July 2000 (21.07.2000) US

(71) Applicant: TELEMAC CORPORATION [US/US]; 6701 Center Drive West, Suite 700, Los Angeles, CA 90045 (US).

(72) Inventors: WATLER, Theodore, W.; 5341 E. 4th Street, Long Beach, CA 90814-1920 (US). HANLEY, Jerry; 1315 Franklin Street, #D, Santa Monica, CA 90404 (US).

(74) Agents: NG, Horace et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

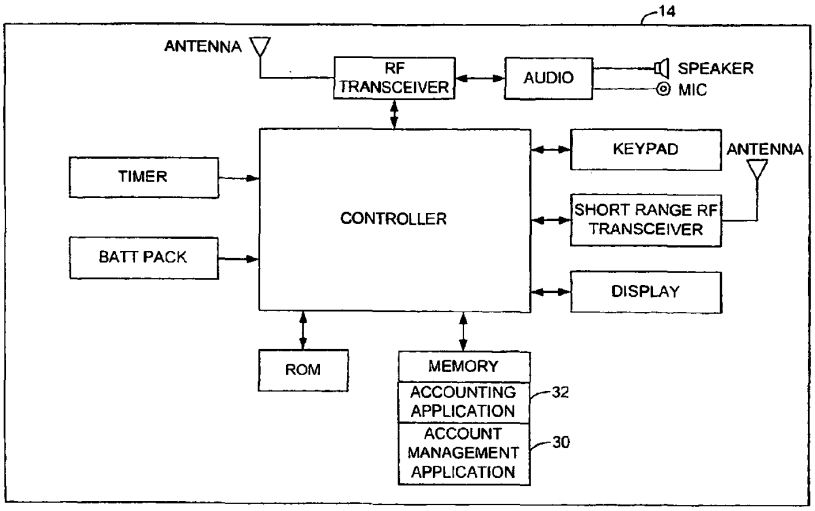
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
30 May 2002

[Continued on next page]

(54) Title: MULTIPLE VIRTUAL WALLETS IN WIRELESS DEVICES



(57) Abstract: A system having a wireless device (14) capable of monitoring and tracking its own usage and account activities is disclosed. The wireless device (14) includes an account management application (30) and accounting applications (32). The account management application (30) manages a variety of accounts in conjunction with the accounting applications (32) and is used by a user to determine how each call/transaction is to be paid for. For example, the user of the wireless device (14) may wish to pay for business calls using a first account and personal calls using a second account.

WO 02/08863 A3

BNSDOCID: <WO_____0208863A3_I_>

IPR2025-01572
Apple EX1002 Page 556

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.

BNSDOCID: <WO_____0208863A3_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/23226

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04M 15/00
US CL : 455/405, 406, 407, 408; 379/114.26

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)
U.S. : 455/405, 406, 407, 408, 409, 422, 575; 379/114.01, 114.03, 114.26

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,774,533 A (PATEL) 30 June 1998 (30.06.1998), column 7, lines 8-31, column 17, line 57 - column 18, line 19, and figure 3.	1-45
Y	US 5,956,653 A (LAHTI) 21 September 1999 (21.09.1999), column 2, lines 7-38, and figure 1.	1-45
Y	US 5,428,666 A (FYFE et al) 27 June 1995 (27.06.1995), column 3, line 59 - column 7, line 36, and figures 1-2.	1-45
Y	US 5,109,401 A (HATTORI et al) 28 April 1992 (28.04.1992), see abstract, column 5, line 56 - column 6, line 56, and figure 3.	14, 24, 43, 44
A	US 5,657,373 A (HERMANSSON et al) 12August 1997 (12.08.1997), column 4,l ine 2 - column 5, line 2.	1-45

☐ 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 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
17 September 2001 (17.09.2001)	22 JAN 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Quochien Vuong Telephone No. (703) 306-4530

Form PCT/ISA/210 (second sheet) (July 1998)

BNSDOCID: <WO_____0208863A3_I_>

IPR2025-01572
Apple EX1002 Page 558

Electronic Acknowledgement Receipt	
EFS ID:	30055056
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	11-AUG-2017
Filing Date:	06-OCT-2016
Time Stamp:	13:35:19
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)	P041D1C1_IDS.pdf	1054583 1002ba567337350d7a0bd4cb234396b4fe0f5cf2	no	6
Warnings:					

Information:					
2	Foreign Reference	2094.pdf	3952944 dfa7cbac15ff6f3701105acf137953f96f215840	no	25
Warnings:					
Information:					
			Total Files Size (in bytes):	5007527	

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1	4727

106963 7590 11/06/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
11/06/2017	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):

patent@headwaterllc.com

Office Action Summary	Application No. 15/287,597	Applicant(s) RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *June 9, 2017*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *2-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *2-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, 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.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ 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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

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

Claims

2. Applicant cancelled claim 1 from the June 9, 2017 Amendment.

3. Claims 2-20 are pending.

Claim Rejections - 35 USC § 101.

4. Claims 2-20 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLtweS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 2-20 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 1, line 7, the phrase “a secure device credential" appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures.

Claim 1, lines 8-9, the phrase “one or more device identifiers of the first device" appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures.

Claim 1, line 12, the phrase “a second request" appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures. As such it is not clear as to the metes and bounds of what this first computing device comprises. Specific clarification where such is found from the original filed application is required.

Claim 1, line 14, the phrase “a second request" appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures.

Claim 1, lines 15-16, the phrase “a secured application credential, for any first application identified from a plurality of device applications registered to use wireless network communications" appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures.

Claim 1, line 17, the phrase “a general application credential for the first application" appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures.

Claim 1, line 20, the phrase “a first secured application credential unique to the first device" appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures.

The above issues present issues that make it not clear as to the metes and bounds of what this claim language comprises. Specific clarification where such is found from the original filed application is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 2-20, as understood, are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Lortz et al., US 8,146,142.

Lortz discloses a trusted secure wireless network system, e.g. Figs. 1-10, using a plurality of devices, a first and second request, e.g. Fig. 6, and a credential policy, e.g. 306. Lotz does not specifically disclose the terms a secured application credential, nor a general application credential. However, these types of credentials would be within

the realm of the Lotz credential policy in order to operate their system over the disclosed network. Official Notice is taken that different application credentials as recited by Applicant used in a secure communication network has been common knowledge in the network system art. To have provided such for Lotz would have been obvious to one of ordinary skill in the art in view of this common knowledge. The motivation for having done such would have been to incorporate this common knowledge used with the arrangement of Lotz for providing a secure communication over a network.

10. Pertinent references of interest are noted on the attached PTO-892.

11. Applicant's seven (7) Information Disclosure Statements (IDS's) have been reviewed. Note the attached IDS's.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Fahd Obeid, can be reached on 571-270-3324. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/

Primary Examiner

Art Unit 3687

Notice of References Cited	Application/Control No. 15/287,597	Applicant(s)/Patent Under Reexamination RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-9,589,117 B2	03-2017	Ali; Valiuddin	G06F21/31	1/1
*	B	US-8,700,729 B2	04-2014	Dua; Robin	G06Q20/20	705/64
*	C	US-8,639,215 B2	01-2014	McGregor; Gregory M.	G06Q20/32	455/406
*	D	US-8,285,992 B2	10-2012	Mathur; Saurabh	H04L63/0236	380/270
*	E	US-8,214,890 B2	07-2012	Kirovski; Darko	H04L9/3073	726/12
*	F	US-8,190,087 B2	05-2012	Fisher; Michelle	G06Q20/102	235/380
*	G	US-8,166,554 B2	04-2012	John; Pramod	H04L63/105	726/26
*	H	US-8,146,142 B2	03-2012	Lortz; Victor B.	G06F21/43	726/26
*	I	US-8,091,087 B2	01-2012	Ali; Abid	G06F11/1461	718/100
*	J	US-7,539,862 B2	05-2009	Edgett; Jeff Steven	H04L63/08	709/223
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	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 MM-YYYY format are publication dates. Classifications may be US or foreign.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	20020022472		2002-02-21	WATLER et al.	
	2	20020120540		2002-08-29	KENDE et al.	
	3	20020131404		2002-09-19	MEHTA et al.	
	4	20020138601		2002-09-26	PIPONIUS et al.	
	5	20020176377		2002-11-28	HAMILTON, Thomas E.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	6	20020199001		2002-12-26	WENOCUR et al.	
	7	20030004937		2003-01-02	SALMENKAITA et al.	
	8	20030005112		2003-01-02	KRAUTKREMER, Todd Joseph	
	9	20030013434		2003-01-16	ROSENBERG et al.	
	10	20030018524		2003-01-23	FISHMAN et al.	
	11	20030046396		2003-03-06	RICHTER et al.	
	12	20030050070		2003-03-13	MASHINSKY et al.	
	13	20030050837		2003-03-13	KIM, Do Sik	
	14	20030088671		2003-05-08	KLINKER et al.	
	15	20030133408		2003-07-17	CHENG et al.	
	16	20030161265		2003-08-28	CAO et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	17	20030182420		2003-09-25	JONES et al.	
	18	20030182435		2003-09-25	REDLICH et al.	
	19	20030220984		2003-11-27	JONES et al.	
	20	20030224781		2003-12-04	MILFORD et al.	
	21	20030229900		2003-12-11	REISMAN, Richard	
	22	20030236745		2003-12-25	HARTSELL et al.	
	23	20040019539		2004-01-29	RAMAN et al.	
	24	20040021697		2004-02-05	BEATON et al.	
	25	20040030705		2004-02-12	BOWMAN-AMUAH, Michel K.	
	26	20040044623		2004-03-04	WAKE et al.	
	27	20040047358		2004-03-11	CHEN et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	28	20040073672		2004-04-15	FASCENDA, Anthony C.	
	29	20040082346		2004-04-29	SKYTT et al.	
	30	20040098715		2004-05-20	AGHERA et al.	
	31	20040103193		2004-05-27	PANDYA et al.	
	32	20040107360		2004-06-03	HERRMANN et al.	
	33	20040127200		2004-07-01	SHAW et al.	
	34	20040132427		2004-07-08	LEE et al.	
	35	20040168052		2004-08-26	CLISHAM et al.	
	36	20040198331		2004-10-07	COWARD et al.	
	37	20040236547		2004-11-25	RAPPAPORT et al.	
	38	20040249918		2004-12-09	SUNSHINE, Roger N.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	39	20050021995		2005-01-27	LAL et al.	
	40	20050048950		2005-03-03	MORPER, Hans-Jochen	
	41	20050055291		2005-03-10	BEVENTE et al.	
	42	20050055309		2005-03-10	WILLIAMS et al.	
	43	20050060266		2005-03-17	DEMELLO et al.	
	44	20050097516		2005-05-05	DONNELLY et al.	
	45	20050107091		2005-05-19	VANNITHAMBY et al.	
	46	20050128967		2005-06-16	SCOBBIE, Donald MacGregor	
	47	20050166043		2005-07-28	ZHANG et al.	
	48	20050183143		2005-08-18	ANDERHOLM et al.	
	49	20050198377		2005-09-08	FERGUSON et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	50	20050216421		2005-09-29	BARRY et al.	
	51	20050228985		2005-10-13	YLIKOSKI et al.	
	52	20050238046		2005-10-27	HASSAN et al.	
	53	20050246282		2005-11-03	NASLUND et al.	
	54	20050250508		2005-11-10	GUO et al.	
	55	20050254435		2005-11-17	MOAKLEY et al.	
	56	20050266825		2005-12-01	CLAYTON, Steve	
	57	20050266880		2005-12-01	GUPTA, Vivek G.	
	58	20060014519		2006-01-19	MARSH et al.	
	59	20060019632		2006-01-26	CUNNINGHAM et al.	
	60	20060026679		2006-02-02	ZAKAS, Philip H.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	61	20060034256		2006-02-16	ADDAGATLA et al.	
	62	20060040642		2006-02-23	BORIS et al.	
	63	20060045245		2006-03-02	AARON et al.	
	64	20060048223		2006-03-02	LEE et al.	
	65	20060072646		2006-04-06	FEHER, Kamilo	
	66	20060085543		2006-04-20	HRASTAR et al.	
	67	20060112016		2006-05-25	ISHIBASHI, Yoshihito	
	68	20060143098		2006-06-29	LAZARIDIS, Mihal	
	69	20060165060		2006-07-27	DUA, Robin	
	70	20060178917		2006-08-10	MERRIAM et al.	
	71	20060178918		2006-08-10	MIKURAK, Michael G.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	72	20060183462		2006-08-17	KOLEHMAINEN, Mikko	
	73	20060190314		2006-08-24	HERNANDEZ, Rick	
	74	20060199608		2006-09-07	DUNN et al.	
	75	20060206904		2006-09-14	WATKINS et al.	
	76	20060218395		2006-09-28	MAES, Stephane H.	
	77	20060233108		2006-10-19	KRISHNAN, Murali R.	
	78	20060233166		2006-10-19	BOU-DIAB et al.	
	79	20060236095		2006-10-19	SMITH et al.	
	80	20060242685		2006-10-26	HEARD et al.	
	81	20060258341		2006-11-16	MILLER et al.	
	82	20060291477		2006-12-28	CROAK et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	83	20070019670		2007-01-25	FALARDEAU, Eric	
	84	20070022289		2007-01-25	ALT et al.	
	85	20070036312		2007-02-15	CAI et al.	
	86	20070055694		2007-03-08	RUGE et al.	
	87	20070061243		2007-03-15	RAMER et al.	
	88	20070076616		2007-04-05	NGO et al.	
	89	20070093243		2007-04-26	KAPADEKAR et al.	
	90	20070100981		2007-05-03	ADAMCZYK et al.	
	91	20070101426		2007-05-03	LEE et al.	
	92	20070104126		2007-05-10	CALHOUN et al.	
	93	20070130315		2007-06-07	FRIEND et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	94	20070140113		2007-06-21	GEMELOS, Steven	
	95	20070140275		2007-06-21	BOWMAN et al.	
	96	20070198656		2007-08-23	MAZZAFERRI et al.	
	97	20070220251		2007-09-20	ROSENBERG et al.	
	98	20070226225		2007-09-27	YIU et al.	
	99	20070243862		2007-10-18	COSKUN et al.	
	100	20070248100		2007-10-25	ZUBERI et al.	
	101	20070254675		2007-11-01	ZORLU OZER et al.	
	102	20070255848		2007-11-01	SEWALL et al.	
	103	20070259673		2007-11-08	WILLARS et al.	
	104	20070263558		2007-11-15	SALOMONE, Leonardo	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	105	20070274327		2007-11-29	KAARELA et al.	
	106	20070282896		2007-12-06	WYDROUG et al.	
	107	20070294395		2007-12-20	STRUB et al.	
	108	20070298764		2007-12-27	CLAYTON, Steve	
	109	20080005285		2008-01-03	ROBINSON et al.	
	110	20080005561		2008-01-03	BROWN et al.	
	111	20080010452		2008-01-10	HOLTZMAN et al.	
	112	20080039102		2008-02-14	SEWALL et al.	
	113	20080049630		2008-02-28	KOZISEK et al.	
	114	20080052387		2008-02-28	HEINZ et al.	
	115	20080059474		2008-03-06	LIM, Keng	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	116	20080059743		2008-03-06	BYCHKOV et al.	
	117	20080060066		2008-03-06	WYNN et al.	
	118	20080062900		2008-03-13	RAO, Bindu Rama	
	119	20080064367		2008-03-13	NATH et al.	
	120	20080066149		2008-03-13	LIM, Keng	
	121	20080066150		2008-03-13	LIM, Keng	
	122	20080082643		2008-04-03	STORRIE et al.	
	123	20080083013		2008-04-03	SOLIMAN et al.	
	124	20080095339		2008-04-24	ELLIOTT et al.	
	125	20080098062		2008-04-24	BALIA, Hinal K.	
	126	20080109679		2008-05-08	WRIGHT et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	127	20080120688		2008-05-22	QIU et al.	
	128	20080127304		2008-05-29	GINTER et al.	
	129	20080130534		2008-06-05	TOMIOKA, Tazuko	
	130	20080130656		2008-06-05	KIM et al.	
	131	20080132268		2008-06-05	CHOI-GROGAN et al.	
	132	20080134330		2008-06-05	KAPOOR et al.	
	133	20080147454		2008-06-19	WALKER et al.	
	134	20080160958		2008-07-03	ABICHANDANI et al.	
	135	20080162637		2008-07-03	ADAMCZYK et al.	
	136	20080162704		2008-07-03	POPLETT et al.	
	137	20080164304		2008-07-10	NARASIMHAN et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	138	20080167027		2008-07-10	GAUTIER et al.	
	139	20080167033		2008-07-10	BECKERS, Michel	
	140	20080168523		2008-07-10	ANSARI et al.	
	141	20080177998		2008-07-24	APSANGI et al.	
	142	20080183812		2008-07-31	PAUL et al.	
	143	20080184127		2008-07-31	RAFEY et al.	
	144	20080189760		2008-08-07	ROSENBERG et al.	
	145	20080207167		2008-08-28	BUGENHAGEN, Michael K.	
	146	20080212470		2008-09-04	CASTANEDA et al.	
	147	20080221951		2008-09-11	STANFORTH et al.	
	148	20080222692		2008-09-11	ANDERSSON et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	149	20080225748		2008-09-18	KHEMANI et al.	
	150	20080229385		2008-09-18	FEDER et al.	
	151	20080229388		2008-09-18	MAES, Stephane H.	
	152	20080256593		2008-10-16	VINBERG et al.	
	153	20080268813		2008-10-30	MAES, Stephane H.	
	154	20080298230		2008-12-04	LUFT et al.	
	155	20080305793		2008-12-11	GALLAGHER et al.	
	156	20080311885		2008-12-18	DAWSON et al.	
	157	20080316923		2008-12-25	FEDDERS et al.	
	158	20080318547		2008-12-25	BALLOU et al.	
	159	20080318550		2008-12-25	DeATLEY, Dallas	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	160	20080319879		2008-12-25	CARROLL et al.	
	161	20090005005		2009-01-01	FORSTALL et al.	
	162	20090013157		2009-01-08	BEAULE, Stephane	
	163	20090054030		2009-02-26	GOLDS, David	
	164	20090068984		2009-03-12	BURNETT, R. Alan	
	165	20090077622		2009-03-19	BAUM et al.	
	166	20090079699		2009-03-26	SUN, Jian	
	167	20090113514		2009-04-30	HU, Q. James	
	168	20090125619		2009-05-14	ANTANI, Snehal S.	
	169	20090180391		2009-07-16	PETERSEN et al.	
	170	20090197585		2009-08-06	AARON, Jeffrey A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	171	20090257379		2009-10-15	ROBINSON et al.	
	172	20090271514		2009-10-29	THOMAS et al.	
	173	20090286507		2009-11-19	O'NEIL et al.	
	174	20090287921		2009-11-19	ZHU et al.	
	175	20090288140		2009-11-19	HUBER et al.	
	176	20100017506		2010-01-21	FADELL, Anthony	
	177	20100042675		2010-02-18	FUJII, Hiroshi	
	178	20100043068		2010-02-18	VARADHAN et al.	
	179	20100071053		2010-03-18	ANSARI et al.	
	180	20100082431		2010-04-01	RAMER et al.	
	181	20100103820		2010-04-29	FULLER et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	182	20100188975		2010-07-29	RALEIGH, Gregory G.	
	183	20100188990		2010-07-29	RALEIGH, Gregory G.	
	184	20100188992		2010-07-29	RALEIGH, Gregory G.	
	185	20100188994		2010-07-29	RALEIGH, Gregory G.	
	186	20100191576		2010-07-29	RALEIGH, Gregory G.	
	187	20100191612		2010-07-29	RALEIGH, Gregory G.	
	188	20100191846		2010-07-29	RALEIGH, Gregory G.	
	189	20100192170		2010-07-29	RALEIGH, Gregory G.	
	190	20100192212		2010-07-29	RALEIGH, Gregory G.	
	191	20100195503		2010-08-05	RALEIGH, Gregory G.	
	192	20100197268		2010-08-05	RALEIGH, Gregory G.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	193	20100198698		2010-08-05	RALEIGH et al.	
	194	20100198939		2010-08-05	RALEIGH, Gregory G.	
	195	20100325420		2010-12-23	KANEKAR, Tushar	
	196	20110126141		2011-05-26	KING et al.	
	197	20080132201		2008-06-05	KARLBERG, Johan	
	198	20080081606		2008-04-03	COLE, Terry L.	
	199	20090248883		2009-10-01	SURYANARAYANA et al.	
	200	20100144310		2010-06-10	BEDINGFIELD, James Carlton	
	201	20080085707		2008-04-10	FADELL, Tony	
	202	20090046723		2009-02-19	RAHMAN, Reshad A. et al.	
	203	20080219268		2008-09-11	DENNISON, Larry R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	204	20080005285		2008-01-03	ROBINSON, James David et al.	
	205	20090315735		2009-12-24	BHAVANI, Neeraj S. et al.	
	206	20090219170		2009-09-03	CLARK, Ryan C. et al.	
	207	20090067372		2009-03-12	SHAH, Keyur C. et al.	
	208	20080262798		2008-10-23	KIM, Eun Ah et al.	
	209	20100103820		2010-04-29	FULLER, Randy et al.	
	210	20100153781		2010-06-17	HANNA, Stephen R.	
	211	20120029718		2012-02-02	DAVIS, Edward L.	
	212	20110241624		2011-10-06	PARK, Jun-seok et al.	
	213	20090307746		2009-12-10	DI, Jinwen et al.	
	214	20050009499		2005-01-13	KOSTER, Karl	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	215	20010053694		2001-12-20	IGARASHI, Yoichiro et al.	
	216	20100041364		2010-02-18	LOTT, Robert Wayne et al.	
	217	20100027469		2010-02-04	GURAJALA, Ravindra Babu et al.	
	218	20090299857		2009-12-03	BRUBAKER, Curtis M.	
	219	20080051076		2008-02-28	O'Shaughnessy, John et al.	
	220	20080313730		2008-12-18	Iftimie, Sorin et al.	
	221	20110173678		2011-07-14	KAIPPALLIMALIL, John et al.	
	222	20080235511		2008-09-25	O'BRIEN, William G. et al.	
	223	20080240373		2008-10-02	WILHELM, Robert D.	
	224	20100027559		2010-02-04	LIN, Hung-Ming et al.	
	225	20020116338		2002-08-22	GONTHIER, Jean-Charles et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	226	20070061878		2007-03-15	HAGIU, Costin et al. et al.	
	227	20100020822		2010-01-28	ZERILLO, Anthony J. et al.	
	228	20040203755		2004-10-14	BRUNET, Jeffrey et al.	
	229	20090172077		2009-07-02	ROXBURGH, David et al.	
	230	20080120668		2008-05-22	Yau, Frank Chuen-Foo	
	231	20030171112		2003-09-11	Lupper, Alfred et al.	
	232	20070300252		2007-12-27	Acharya, Swarup et al.	
	233	20050007993		2005-01-13	Chambers, Mahdi et al.	
	234	20020164983		2002-11-07	Raviv, Li-On et al.	
	235	20070280453		2007-12-06	Kelley, Sean S.	
	236	20100241544		2010-09-23	Benson, Dan et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	237	20090157792		2009-06-18	Fiatal, Trevor	
	238	20070109983		2007-05-17	Shankar, Rohit et al.	
	239	20020049074		2002-04-25	Eisinger, Bernd et al.	
	240	20020161601		2002-10-31	Nauer, Bernhard et al.	
	241	20040132427		2004-07-08	Lee, Wan-Yeon et al.	
	242	20060068796		2006-03-30	Millen, Stephanie L. et al.	
	243	20010048738		2001-12-06	Baniak, Paul G. et al.	
	244	20070033197		2007-02-08	Scherzer, Shimon et al.	
	245	20110013569		2011-01-20	Scherzer, Shimon et al.	
	246	20110159818		2011-06-30	Scherzer, Shimon et al.	
	247	20120020296		2012-01-26	Scherzer, Shimon et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	248	20120196644		2012-08-02	Scherzer, Shimon et al.	
	249	20120238287		2012-09-20	Scherzer, Shimon	
	250	20130058274		2013-03-07	Scherzer, Shimon et al.	
	251	20130084835		2013-04-04	Scherzer, Shimon et al.	
	252	20090005000		2009-01-01	Baker, Matthew et al.	
	253	20090006116		2009-01-01	Baker, Matthew et al.	
	254	20090006200		2009-01-01	Baker, Matthew et al.	
	255	20110081881		2011-04-07	Baker, Matthew Donald et al.	
	256	20110082790		2011-04-07	Baker, Matthew Donald et al.	
	257	20130029653		2013-01-31	Baker, Matthew Donald et al.	
	258	20130065555		2013-03-14	Baker, Matthew Donald et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	259	20120155296		2012-06-21	Kashanian, Nematolah	
	260	20120330792		2012-12-27	Kashanian, Nematolah	
	261	20130030960		2013-01-31	Kashanian, Nematolah	
	262	20130095787		2013-04-18	Kashanian, Nematolah	
	263	20130117140		2013-05-09	Kashanian, Nematolah	
	264	20130183937		2013-07-18	Neal, Daniel John et al.	
	265	20060135144		2006-06-22	Jothipragasam, Premkumar	
	266	20080089295		2008-04-17	Keeler, James D. et al.	
	267	20080022354		2008-01-24	Grewal, Karanvir et al.	
	268	20040102182		2004-05-27	Reith, Lothar et al.	
	269	20030233332		2003-12-18	Keeler, James D. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	270	20080250053		2008-10-09	Aaltonen, Janne et al.	
	271	20110195700		2011-08-11	Kukuchka, Robert et al.	
	272	20070155365		2007-07-05	Kim, Sung-Jun et al.	
	273	20130144789		2013-06-06	Aaltonen, Janne et al.	
	274	20100131584		2010-05-27	Johnson, William J.	
	275	20100080202		2010-04-01	Hanson, Mark	
	276	20070147324		2007-06-28	McGary, Faith	
	277	20130024914		2013-01-24	Ahmed, Shahid et al.	
	278	20130103376		2013-04-25	Gaddam, Venkat et al.	
	279	20130111572		2013-05-02	Gaddam, Venkat et al.	
	280	20130117382		2013-05-09	Gaddam, Venkat et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	281	20130149994		2013-06-13	Gaddam, Venkat et al.	
	282	20070168499		2007-07-19	Chu, Jing-Long	
	283	20070025301		2007-02-01	Petersson, Justus et al.	
	284	20070140145		2007-06-21	Kumar, Surender et al.	
	285	20080120129		2008-05-22	Seubert, Michael et al.	
	286	20060174035		2006-08-03	Tufail, Mudassir	
	287	20110264923		2011-10-27	Kocher, Paul C. et al.	
	288	20080201266		2008-08-21	Chua, Huina et al.	
	289	20060156398		2006-07-13	Ross, Alan D. et al.	
	290	20060173959		2006-08-03	McKelvie, Samuel J. et al.	
	291	20100284327		2010-11-11	Miklos, Gyorgy	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	292	20070033194		2007-02-08	Srinivas, Davanum M. et al.	
	293	20050079863		2005-04-14	Macaluso, Anthony G.	
	294	20060114832		2006-06-01	Hamilton, Thomas E. et al.	
	295	20040225898		2004-11-11	Frost, D. Gabriel et al.	
	296	20080070550		2008-03-20	Hose, David Alan	
	297	20110019574		2011-01-27	Malomsoky, Szaboles et al.	
	298	20030188117		2003-10-02	Yoshino, Kenji et al.	
	299	20040255145		2004-12-16	Chow, Jerry	
	300	20050055595		2005-03-10	Frazer, Mark et la.	

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]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	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]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	10/10/2017

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

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

BIB DATA SHEET

CONFIRMATION NO. 4727

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/287,597	10/06/2016	705	3687	RALEP041D1C1

APPLICANTS

Headwater Partners I LLC, Tyler, TX;

INVENTORS

Gregory G. Raleigh, Woodside, CA;
Jeffrey Green, Sunnyvale, CA;
James Lavine, Corte Madera, CA;

**** CONTINUING DATA ***************************

This application is a CON of 14/340,270 07/24/2014 PAT 9491199
which is a DIV of 13/309,463 12/01/2011 PAT 8793758
which claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/550,906 10/24/2011
and is a CIP of 13/237,827 09/20/2011 PAT 8832777
and is a CIP of 13/134,028 05/25/2011 PAT 8589541
and is a CIP of 13/253,013 10/04/2011 PAT 8745191
and said 13/237,827 09/20/2011
claims benefit of 61/384,456 09/20/2010
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
which claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028 05/25/2011
claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/407,358 10/27/2010
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and said 12/694,455 01/27/2010
claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
claims benefit of 61/252,153 10/15/2009
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/134,005 05/25/2011
is a CIP of 12/380,778 03/02/2009 PAT 8321526

IPR2025-01572
Apple EX1002 Page 598

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Gregory G. Raleigh
Art Unit	2431
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	6219786	B1	2001-04-17	Cunningham et al.	

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	20060020787	A1	2006-01-26	Choyi et al.	
	2	20060072550	A1	2006-04-06	Davis et al.	
	3	20060190987	A1	2006-08-24	Ohta et al.	
	4	20080077705	A1	2008-03-27	Li et al.	
	5	20080259924	A1	2008-10-23	Gooch et al.	

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

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2431
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

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	2005053335	WO	A1	2005-06-09	Nokia Corp.		

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		

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	10/10/2017

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP041D1C1

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	6466984	B1	2002-10-15	Naveh et al.	
	2	6522629	B1	2003-02-18	Anderson, Sr., Ronald D.	
	3	6996062	B1	2006-02-07	Freed et al.	
	4	7269157	B2	2007-09-11	Klinker et al.	
	5	7340772	B2	2008-03-04	Panasyuk et al.	
	6	7423971	B1	2008-09-09	Mohaban et al.	
	7	7522576	B2	2009-04-21	Du et al.	
	8	7769397	B2	2010-08-03	Funato et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	9	7882247	B2	2011-02-01	Sturniolo et al.	
	10	7925740	B2	2011-04-12	Nath et al.	
	11	8010990	B2	2011-08-30	Ferguson et al.	
	12	8159520	B1	2012-04-17	Dhanoa et al.	
	13	8446831	B2	2013-05-21	Kwan et al.	
	14	8499087	B2	2013-07-30	Hu, Qingmin	
	15	8619735	B2	2013-12-31	Montemurro et al.	
	16	8826411	B2	2014-09-02	Moen et al.	
	17	9015331	B2	2015-04-21	Lai et al.	
	18	9402254	B2	2016-07-26	Kneckt et al.	
	19	9634850	B2	2017-04-25	Taft et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

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	20050111463	A1	2005-05-26	Leung et al.	
	2	20090149154	A1	2009-06-11	Bhasin et al.	
	3	20090291665	A1	2009-11-26	Gaskarth et al.	
	4	20110177811	A1	2011-07-21	Heckman et al.	

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	0208863	WO		2002-01-31	Telemac Corp.		

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		

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	10/10/2017

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	7260382		2007-08-21	Lamb et al.	
	2	7685530		2010-03-23	Sherrard et al.	
	3	7937450		2011-05-03	Janik, Craig M.	
	4	8019846		2011-09-13	Roelens et al.	
	5	8050705		2011-11-01	Sicher et al.	
	6	8086791		2011-12-27	Caulkins, Jason	
	7	7627872		2009-12-01	Hebeler et al.	
	8	8532610		2013-09-10	Manning Cassett et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	8631428		2014-01-14	Scott et al.	
	10	8804517		2014-08-12	Oerton, Kevin John	
	11	8949597		2015-02-03	Reeves et al.	
	12	8831561		2014-09-09	Sutaria et al.	
	13	8010082		2011-08-30	Sutaria et al.	
	14	7271765		2007-09-18	Stilp et al.	
	15	7843843		2010-11-30	Papp III et al.	
	16	8495181		2013-07-23	Venkatraman et al.	
	17	9049010		2015-06-02	Jueneman et al.	
	18	8174378		2012-05-08	Richman et al.	
	19	6757717		2004-06-29	Goldstein, Leonid	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	7007295		2006-02-28	Rose et al.	
	21	8208788		2012-06-26	Ando et al.	
	22	8326828		2012-12-04	Zhou et al.	
	23	8761711		2014-06-24	Grignani et al.	
	24	7222190		2007-05-22	Klinker, Eric et al.	
	25	8713535		2014-04-29	Malhotra et al.	
	26	5572528		1996-11-05	Shuen, Pauline	
	27	5754953		1998-05-19	Briancon et al.	
	28	6628934		2003-09-30	Rosenberg et al.	
	29	6662014		2003-12-09	Walsh, Patrick Jay	
	30	6901440		2005-05-31	Bimm et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	31	6970692		2005-11-29	Tysor, Arthur James	
	32	7203752		2007-04-10	Rice et al.	
	33	7224968		2007-05-29	Dobson et al.	
	34	7379731		2008-05-27	Natsuno et al.	
	35	7457870		2008-11-25	Lownsbrough et al.	
	36	7515926		2009-04-07	Bu et al.	
	37	7536695		2009-05-19	Alam et al.	
	38	7586871		2009-09-08	Hamilton et al.	
	39	7752330		2010-07-06	Olsen et al.	
	40	7792257		2010-09-07	Vanier et al.	
	41	7801783		2010-09-21	Kende et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	42	7865187		2011-01-04	Ramer et al.	
	43	7933274		2011-04-26	Verma et al.	
	44	8005726		2011-08-23	Bao, Yulin	
	45	8050690		2011-11-01	Neeraj, Chawla	
	46	8086398		2011-12-27	Sanchez et al.	
	47	8107953		2012-01-31	Zimmerman et al.	
	48	8112435		2012-02-07	Epstein et al.	
	49	8195661		2012-06-05	Kalavade, Asawaree	
	50	8200163		2012-06-12	Hoffman, George E.	
	51	8200818		2012-06-12	Freund et al.	
	52	8254880		2012-08-28	Aaltonen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	53	8270955		2012-09-18	Ramer et al.	
	54	8331223		2012-12-11	Hill et al.	
	55	8358975		2013-01-22	Bahl et al.	
	56	8533775		2013-09-10	Alcorn et al.	
	57	8538394		2013-09-17	Zimmerman et al.	
	58	8538458		2013-09-17	Haney, Richard D.	
	59	8565746		2013-10-22	Hoffman, George E.	
	60	8571501		2013-10-29	Miller et al.	
	61	8644702		2014-02-04	Kalajan, Kevin E.	
	62	8713641		2014-04-29	Pagan et al.	
	63	8730842		2014-05-20	Collins et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	64	8732808		2014-05-20	Sewall et al.	
	65	6445777		2002-09-03	Clark, Curtis	
	66	7039027		2006-05-02	Bridgelall, Raj	
	67	7990049		2011-08-02	Shioya, Shunsuke	
	68	8180886		2012-05-15	Overcash et al.	
	69	8339991		2012-12-25	Biswas et al.	
	70	8630314		2014-01-14	York, Frederick John	
	71	8868725		2014-10-21	Samba, Augustine S.	
	72	7149521		2006-12-12	Sundar et al.	
	73	7200112		2007-04-03	Sundar et al.	
	74	7395244		2008-07-01	Kingsford, Bryan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	75	7411930		2008-08-12	Montojo, Juan et al.	
	76	7508799		2009-03-24	Sumner et al.	
	77	7554983		2009-06-30	Muppala, Suresh	
	78	7564799		2009-07-21	Holland et al.	
	79	7849477		2010-12-07	Cristofalo et al.	
	80	7987496		2011-07-26	Bryce et al.	
	81	8503455		2013-08-06	Heikens, Heico	
	82	RE44412		2013-08-06	Naqvi et al.	
	83	8484568		2013-07-09	Rados et al.	
	84	5974439		1999-10-26	Bollella, Gregory	
	85	6882718		2005-04-19	Smith, Benjamin V.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	86	7058022		2006-06-06	Carolan et al.	
	87	7017189		2006-03-21	DeMello et al.	
	88	7266371		2007-09-04	Amin et al.	
	89	8190122		2012-05-29	Alexander et al.	
	90	9002342		2015-04-07	Tenhunen et al.	
	91	8385964		2013-02-26	Haney, Richard D.	
	92	8504032		2013-08-06	Lott et al.	
	93	7366654		2008-04-29	Moore, Robert C.	
	94	7391724		2008-06-24	Alakoski et al.	
	95	7978686		2011-07-12	Goyal et al.	
	96	8644813		2014-02-04	Gailloux et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	97	6393014		2002-05-21	Daly et al.	
	98	6397259		2002-05-28	Lincke et al.	
	99	7047276		2006-05-16	Liu et al.	
	100	7627767		2009-12-01	Sherman et al.	
	101	7849161		2010-12-07	Koch et al.	
	102	7894431		2011-02-22	Goring et al.	
	103	8073427		2011-12-06	Koch et al.	
	104	8522337		2013-08-27	Adusumilli et al.	
	105	8527662		2013-09-03	Biswas et al.	
	106	8572256		2013-10-29	Babbar, Uppinder Singh	
	107	8966018		2015-02-24	Bugwadia et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	108	7162237		2007-01-09	Silver et al.	
	109	7454191		2008-11-18	Dawson et al.	
	110	7817615		2010-10-19	Breau et al.	
	111	7844034		2010-11-30	Oh et al.	
	112	7899039		2011-03-01	Andreasen et al.	
	113	8104080		2012-01-24	Burns et al.	
	114	8150394		2012-04-03	Bianconi et al.	
	115	8667542		2014-03-04	Bertz et al.	
	116	8793304		2014-07-29	Lu et al.	
	117	8948726		2015-02-03	Smith et al.	
	118	7860088		2010-12-28	Lioy, Marcello	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	119	8812525		2014-08-19	Taylor III, Buford Leonard	
	120	8504690		2013-08-06	Shah et al.	
	121	8407763		2013-03-26	Weller et al.	
	122	8131840		2012-03-06	Denker, Richard E.	
	123	7676673		2010-03-09	Weller et al.	
	124	7512128		2009-03-31	DiMambro et al.	
	125	7248570		2007-07-24	Bahl et al.	
	126	7024460		2006-04-04	Koopmas et al.	
	127	6748437		2004-06-08	Mankude et al.	
	128	6735206		2004-05-11	Oki et al.	
	129	6058434		2000-05-02	Wilt et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	130	8032168		2011-10-04	Ikaheimo, Jorma	
	131	7966405		2011-06-21	Sundaresan et al.	
	132	7889384		2011-02-15	Armentrout et al.	
	133	6125391		2000-09-26	Meltzer et al.	
	134	6038540		2000-03-14	Krist et al.	
	135	8504687		2013-08-06	Maffione et al.	
	136	8863111		2014-10-14	Selitser et al.	
	137	8972537		2015-03-03	Bastian et al.	
	138	9176913		2015-11-03	Millet et al.	
	139	7043225		2006-05-09	Patel et al.	
	140	6725256		2004-04-20	Albal et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	141	6751296		2004-06-15	Albal et al.	
	142	6934751		2005-08-23	Jayapalan et al.	
	143	7174156		2007-02-06	Mangal, Manish	
	144	7636626		2009-12-22	Oesterling et al.	
	145	7720206		2010-05-18	Devolites et al.	
	146	8180333		2012-05-15	Wells et al.	
	147	8340678		2012-12-25	Pandey, Vinod	
	148	8005913		2011-08-23	Carlander, Carrie	
	149	6792461		2004-09-14	Hericourt, Olivier	
	150	7027055		2006-04-11	Anderson et al	
	151	8160056		2012-04-17	Van der Merwe et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	152	5633868		1997-05-27	Baldwin et al.	
	153	7680086		2010-03-16	Eglin, Matthew George	
	154	7765294		2010-07-27	Edwards et al.	
	155	7843831		2010-11-30	Morrill et al.	
	156	8131858		2012-03-06	Agulnik et al.	
	157	8223655		2012-07-17	Heinz et al.	
	158	8385199		2013-02-26	Coward et al.	
	159	8520595		2013-08-27	Yadav et al.	
	160	9135037		2015-09-15	Petrescu-Prahova et al.	
	161	6061571		2000-05-09	Tamura, Hideo	
	162	6157636		2000-12-05	Voit et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	163	7110753		2006-09-19	Campen, Kenneth Brian	
	164	8523547		2013-09-03	Pekrul, Merton W.	
	165	8875042		2014-10-28	Lejeune et al.	
	166	9177455		2015-11-03	Remer, David M.	
	167	8315198		2012-11-20	Corneille et al.	
	168	9172553		2015-10-27	Dawes et al.	
	169	8621056		2013-12-31	Coussemaeker et al.	
	170	7770785		2010-08-10	Jha et al.	
	171	7817983		2010-10-19	Cassett et al.	
	172	8600895		2013-12-03	Felsher, David Paul	
	173	6535855		2003-03-18	Cahill et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	174	6654786		2003-11-25	Fox et al.	
	175	7272660		2007-09-18	Powers et al.	
	176	8065365		2011-11-22	Saxena et al.	
	177	8085808		2011-12-27	Brusca et al.	
	178	8325906		2012-12-04	Fullarton et al.	
	179	8340628		2012-12-25	Taylor et al.	
	180	8448015		2013-05-21	Gerhart, David	
	181	8675852		2014-03-18	Maes, Stephane H.	
	182	8971912		2015-03-03	Chou et al.	
	183	9151205		2012-04-03	Follmann et al.	
	184	7133386		2006-11-07	Holur et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	185	8744339		2014-06-03	Halfmann et al.	
	186	8811338		2014-08-19	Jin et al.	
	187	8908516		2014-12-09	Tzamaloukas et al.	
	188	9030934		2015-05-12	Shah et al.	
	189	7440433		2008-10-21	Rink et al.	
	190	8191106		2012-05-29	Choyi et al.	
	191	6947985		2005-09-20	Hegli et al.	
	192	8195153		2012-06-05	Frencel et al.	
	193	8505073		2013-08-06	Taglienti et al.	
	194	8898748		2014-11-25	Burks et al.	
	195	9282460		2016-03-08	Souissi, Slim Salah	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	196	8995952		2015-03-31	Baker et al.	
	197	8971841		2015-03-03	Menezes et al.	
	198	8538421		2013-09-17	Brisebois et al.	
	199	8503358		2013-08-06	Hanson et al.	
	200	8271025		2012-09-18	Brisebois et al.	
	201	7661124		2010-02-09	Ramanathan et al.	
	202	6141565		2000-10-31	Feurerstein et al.	
	203	6690918		2004-02-10	Evans et al.	
	204	7657920		2010-02-02	Arseneau et al.	
	205	7724716		2010-05-25	Fadell, Anthony M.	
	206	8320902		2012-11-27	Moring et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	207	8837322		2014-09-16	Venkataramanan et al.	
	208	9325737		2016-04-26	Gutowski et al.	
	209	9344557		2016-05-17	Gruchala et al.	
	210	8731519		2014-05-20	Flynn et al.	
	211	8363799		2013-01-29	Gruchala et al.	
	212	6510152		2003-01-21	Gerszberg et al.	
	213	6542500		2003-04-01	Gerszberg et al.	
	214	6546016		2003-04-08	Gerszberg et al.	
	215	6570974		2003-05-27	Gerszberg et al.	
	216	7082422		2006-07-25	Zirngibl et al.	
	217	7369848		2008-05-06	Jiang, Yue Jun	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	218	7577431		2009-08-18	Jiang, Yue Jun	
	219	7664494		2010-02-16	Jiang, Yue Jun	
	220	7873001		2011-01-18	Silver, Andrew	
	221	8219134		2012-07-10	Maharajh et al.	
	222	8291439		2012-10-16	Jethi et al.	
	223	9367680		2016-06-14	Mahaffey et al.	
	224	8670752		2014-03-11	Fan et al.	
	225	9032427		2015-05-12	Gallant et al.	
	226	9173090		2015-10-27	Tuchman et al.	
	227	9367680		2016-06-14	Mahaffey et al.	
	228	6636721		2003-10-21	Threadgill et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	229	7979069		2011-07-12	Hupp et al.	
	230	8145194		2012-03-27	Yoshikawa et al.	
	231	8380247		2013-02-19	Engstrom, G. Eric	
	232	8494559		2013-07-23	Malmi, Robert A.	
	233	8719397		2014-05-06	Levi et al.	
	234	8838752		2014-09-16	Lor et al.	
	235	6959393		2005-10-25	Hollis et al.	
	236	7177919		2007-02-13	Truong et al.	
	237	7369856		2008-05-06	Ovadia, Shlomo	
	238	7428750		2008-09-23	Dunn et al.	
	239	8543814		2013-09-24	Laitinen, et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	240	8700729		2014-04-15	Dua, Robin	
	241	8943551		2015-01-27	Ganapathy et al.	
	242	9413546		2016-08-09	Meier et al.	
	243	5617539		1997-04-01	Ludwig et al.	
	244	6601040		2003-07-29	Kolls, H. Brock	
	245	7486658		2009-02-03	Kumar, Rajneesh	
	246	7602746		2009-10-13	Calhoun et al.	
	247	7599714		2009-10-06	Kuzminskiy, Alexandr	
	248	7610047		2009-10-27	Hicks III et al.	
	249	7643411		2010-01-05	Andreasen et al.	
	250	8194581		2012-06-05	Schroeder et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	251	8787249		2014-07-22	Giaretta et al.	
	252	8862751		2014-10-14	Faccin et al.	
	253	7719966		2010-05-18	Luft et al.	
	254	8132256		2012-03-06	Bari, Farooq	
	255	8307095		2012-11-06	Clark et al.	
	256	8412798		2013-04-02	Wang, Frank C.	
	257	8418168		2013-04-09	Tyhurst et al.	
	258	8838686		2014-09-16	Getchius, Jeffery M.	
	259	8855620		2014-10-07	Sievers et al.	
	260	6401113		2002-06-04	Lazaridis et al.	
	261	7660419		2010-02-09	Ho, Jin-Meng	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	262	8036387		2011-10-11	Kudelski et al.	
	263	8044792		2011-10-25	Orr et al.	
	264	8140690		2012-03-20	Ly et al.	
	265	8639215		2014-01-28	McGregor et al.	
	266	8819253		2014-08-26	Simeloff et al.	
	267	7562213		2009-07-14	Timms, Natalie	
	268	8521775		2013-08-27	Poh et al.	
	269	7151764		2006-12-19	Heinonen et al.	
	270	7191248		2007-03-13	Chattopadhyay et al.	
	271	7095754		2006-08-22	Benveniste, Mathilde	
	272	7136361		2006-11-14	Benveniste, Mathilde	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	273	8402165		2013-03-19	Deu-Ngoc et al.	
	274	7409569		2008-08-05	Illowsky et al.	
	275	8125897		2012-02-28	Ray et al.	
	276	8531954		2013-09-10	McNaughton et al.	
	277	6879825		2005-04-12	Daly, Brian Kevin	
	278	6115823		2000-09-05	Velasco et al.	
	279	7203721		2007-04-10	Ben-Efraim et al.	
	280	7219123		2007-05-15	Fiechter et al.	
	281	7505795		2009-03-17	Lim et al.	
	282	9326173		2016-04-26	Luft, Achim	
	283	7389412		2008-06-17	Sharma et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	284	7466652		2008-12-16	Lau et al.	
	285	7512131		2009-03-31	Svensson et al.	
	286	7526541		2009-04-28	Roese et al.	
	287	8539544		2013-09-17	Garimella et al.	
	288	9111088		2015-08-18	Ghai et al.	

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	1567818A	CN		2005-01-19	Huawei Tech. Co. Ltd.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	2	2006012610	WO		2006-02-02	Citrix Systems, Inc.		
	3	1508734A	CN		2004-06-30	Chinese Creative Corp.		
	4	2688553	CA		2008-12-04	Yoggie Security Systems, Inc.		
	5	1850575	EP		2007-10-31	Research In Motion Limited		
	6	2003017063	WO	A2	2003-02-27	Apogee Networks		
	7	2002067616	WO	A1	2002-08-29	Sonera Oyj		
	8	2011002450	WO	A1	2011-01-06	Alcatel-Lucent USA Inc.		
	9	2003017065	WO	A2	2003-02-27	Apogee Networks		
	10	1545114	EP	A1	2005-06-22	Alcatel		
	11	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	12	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	13	1878160	CN	A	2006-12-13	Huawei Technologies Co., Ltd.		

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.	T5
	1	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	
	2	Kassar et al., "An overview of vertical handover decision strategies in heterogeneous wireless networks," ScienceDirect, University Pierre & Marie Curie, Paris, France, 6/5/2007	
	3	Schiller et al., "Location-Based Services," The Morgan Kaufmann Series in Data Management Systems, 2004	
	4	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	
	5	Jing et al., "Client-Server Computing in Mobile Environments," GTE Labs. Inc., Purdue University, ACM Computing Surveys, Vol. 31, No. 2, June 1999	
	6	Rivadeneyra et al., "A communication architecture to access data services through GSM," San Sebastian, Spain, 1998	
	7	Loopt User Guide, metroPCS, 7/17/2008	
	8	"Jentro Technologies launches Zenlet platform to accelerate location-based content delivery to mobile devices," The Mobile Internet, Boston, MA, Feb. 2008	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	'Ads and movies on the run," the Gold Coast Bulletin, Southport, Qld, Jan. 29, 2008	
	10	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	
	11	Kim, "Free wireless a high-wire act; MetroFi needs to draw enough ads to make service add profits," San Francisco Chronicle, Aug. 21, 2006	
	12	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	
	13	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	
	14	Sabat, "The evolving mobile wireless value chain and market structure," Nov. 2002	
	15	Nuzman et al., "A compund model for TCP connection arrivals for LAN and WAN applications," Oct. 22, 2002	
	16	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	17	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	18	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	19	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	21	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	22	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	
	23	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	24	Roy et al., "Energy Management in Mobile Devices with the Cinder Operating System", Stanford University, MIT CSAIL, June 3, 2010	
	25	Windows7 Power Management, published April 2009	
	26	Quintana, David, "Mobile Multitasking," April 14, 2010	
	27	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	10/10/2017

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	8174970		2012-05-08	Adamczyk, Maria et al.	
	2	8165576		2012-04-24	Raju, Vishwanath et al.	
	3	8073721		2011-12-06	Lewis, Lundy	
	4	8032899		2011-10-04	Archer, Charles J. et al.	
	5	7974624		2011-07-05	Gallagher, Michael D. et al.	
	6	7907970		2011-03-15	Park, Vincent D. et al.	
	7	7778176		2010-08-17	Morford, Michael Robert	
	8	7725570		2010-05-25	Lewis, Lundy	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	7634388		2009-12-15	Archer, Charles J. et al.	
	10	7633438		2009-12-15	Tysowski, Piotr Konrad	
	11	7593417		2009-09-22	Wang, James et al.	
	12	7551922		2009-06-23	Roskowski, Steve et al.	
	13	7545782		2009-06-09	Rayment, Stephen G. et al.	
	14	7039037		2006-05-02	Wang, Jiwei R. et al.	
	15	6928280		2005-08-09	Xanthos, James et al.	
	16	6765925		2004-07-20	Sawyer, Wilson et al.	
	17	5889477		1999-03-30	Fastenrath, Ulrich	
	18	8332517		2012-12-11	Russell, Jesse E.	
	19	8315718		2012-11-20	Caffrey, Paul Oliver et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	8447980		2013-05-21	Godfrey, James A. et al.	
	21	8429403		2013-04-23	Moret, Eric et al.	
	22	8411587		2013-04-02	Curtis, William et al.	
	23	8396929		2013-03-12	Helfman, Nadav et al.	
	24	8363658		2013-01-29	Delker, Jason R. et al.	
	25	8265004		2012-09-11	Toutonghi, Michael J.	
	26	8233895		2012-07-31	Tysowski, Piotr Konrad	
	27	7685254		2010-03-23	Pandya, Ashish A.	
	28	7181017		2007-02-20	Nagel, Robert H. et al.	
	29	6965872		2005-11-15	Grdina, Jerome M.	
	30	8406427		2013-03-26	Chand, Naresh et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	31	8429409		2013-04-23	Wall, Jonathan et al.	
	32	8402540		2013-03-19	Kapoor, Harsh et al.	
	33	8135657		2012-03-13	Kapoor, Harsh et al.	
	34	8271992		2012-09-18	Chatley, Scott P. et al.	
	35	8315999		2012-11-20	Chatley, Scott P. et al.	
	36	8332375		2012-12-11	Chatley, Scott P. et al.	
	37	8468337		2013-06-18	Gaur, Santosh P. et al.	
	38	8477778		2013-07-02	Lehmann Jr., L. Curtis et al.	
	39	8352630		2013-01-08	Hart, Justin Scott	
	40	6640097		2003-10-28	Corrigan, Louis et al.	
	41	7039713		2006-05-02	Van Gunter, David et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	42	5915008		1999-06-22	Dulman, Scott	
	43	8126476		2012-02-28	Vardi, Yosef et al.	
	44	8000276		2011-08-16	Scherzer, Shimon et al.	
	45	8358638		2013-01-22	Scherzer, Tamir et al.	
	46	8356336		2013-01-15	Johnston, Keith et al.	
	47	8307067		2012-11-06	Ryan, Nicholas M.	
	48	7286848		2007-10-23	Vireday, Richard P. et al.	
	49	7313237		2007-12-25	Bahl, Paramvir et al.	
	50	7444669		2008-10-28	Bahl, Paramvir et al.	
	51	7548976		2009-06-16	Bahl, Paramvir et al.	
	52	8027339		2011-09-27	Short, Joel E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	53	8095112		2012-01-10	Chow, Richard et al.	
	54	8369274		2013-02-05	Sawai, Ryo	
	55	7881697		2011-02-01	Baker, Matthew Donald et al.	
	56	7899438		2011-03-01	Baker, Matthew Donald et al.	
	57	7945238		2011-05-17	Baker, Matthew Donald et al.	
	58	8078140		2011-12-13	Baker, Matthew Donald et al.	
	59	8285249		2012-10-09	Baker, Matthew Donald et al.	
	60	7493659		2009-02-17	Wu, Handong et al.	
	61	7801985		2010-09-21	Pitkow, Jim et al.	
	62	8242959		2012-08-14	Mia, Rashidus S. et al.	
	63	8326319		2012-12-04	Davis, Richard W.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	64	8019886		2011-09-13	Harrang, Jeffrey Paul et al.	
	65	7102620		2006-09-05	Harries, Andrew Stanely Guy et al.	
	66	7139569		2006-11-21	Kato, Akira	
	67	7529204		2009-05-05	Bourlas, Yair et al.	
	68	7720960		2010-05-18	Pruss, Richard Manfred et al.	
	69	7969950		2011-06-28	Iyer, Pradeep J. et al.	
	70	8032409		2011-10-04	Mikurak, Michael G.	
	71	8045973		2011-10-25	Chambers, Michael D.	
	72	8116781		2012-02-14	Chen, Xixian et al.	
	73	8126396		2012-02-28	Bennett, James D.	
	74	8351898		2013-01-08	Raleigh, Gregory G.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	75	5630159		1997-05-13	Zancho, William F.	
	76	5633484		1997-05-27	Zancho, William F. et al.	
	77	5814798		1998-09-29	Zancho, William F.	
	78	7039403		2006-05-02	Wong, Gregory A.	
	79	7583964		2009-09-01	Wong, Gregory A.	
	80	7593730		2009-09-22	Khandelwal, Deepak et al.	
	81	7948953		2011-05-24	Melkote, Keerti G. et al.	
	82	8200509		2012-06-12	Kenedy, Andrew Alexander et al.	
	83	8270972		2012-09-18	Otting, Marcia J. et al.	
	84	7929959		2011-04-19	DeAtley, Dallas et al.	
	85	7478420		2009-01-13	Wright, Michael et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	86	7502672		2009-03-10	Kolls, H. Brock	
	87	7756757		2010-07-13	Oakes III, Charles Lee	
	88	7930446		2011-04-19	Kesselman, Alex et al.	
	89	8078163		2011-12-13	Lemond, Eric et al.	
	90	8068829		2011-11-29	Lemond, Eric et al.	
	91	8086497		2011-12-27	Oakes III, Charles Lee	
	92	8166040		2012-04-24	Brindisi, Richard G. et al.	
	93	6934249		2005-08-23	Bertin, Olivier et al.	
	94	7774456		2010-08-10	Lownsbrough, Derek Leigh et al.	
	95	8447607		2013-05-21	Weider, Chris et al.	
	96	8504729		2013-08-06	Pezzutti, David A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	97	8495227		2013-07-23	Kaminsky, David L. et al.	
	98	8472371		2013-06-25	Bari, Farooq et al.	
	99	8134954		2012-03-13	Godfrey, James A. et al.	
	100	7535880		2009-05-19	Hinman, Brian L. et al.	
	101	7499438		2009-03-03	Hinman, Brian L. et al.	
	102	7496652		2009-02-24	Pezzutti, David	
	103	6957067		2005-10-18	Iyer, Pradeep J. et al.	
	104	6654814		2003-11-25	Britton, Kathryn H. et al.	
	105	8374592		2013-02-12	Proctor, Jr. James A. et al.	
	106	8325638		2012-12-04	Jin, Haipeng et al.	
	107	8116749		2012-02-14	Proctor Jr., James Arthur et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	108	8090616		2012-01-03	Proctor Jr., James Arthur et al.	
	109	8090359		2012-01-03	Proctor Jr., James Arthur et al.	
	110	8150431		2012-04-03	Wolovitz, Lionel et al.	
	111	8483135		2013-07-09	Cai, Yigang et al.	
	112	6104700		2000-08-15	Haddock, Stephen R. et al.	
	113	8185127		2012-05-22	Cai, Zheng et al.	
	114	8521110		2013-08-27	Rofougaran, Ahmadreza	
	115	7310424		2007-12-18	Gehring, Stephan Walter et al.	
	116	7356011		2008-04-08	Waters, Christopher J.F. et al.	
	117	7546460		2009-06-09	Maes, Stephane H.	
	118	7921463		2011-04-05	Sood, Kapil et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	119	7940751		2011-05-10	Hansen, Christopher J.	
	120	8122249		2012-02-21	Falk, Rainer et al.	
	121	8495360		2013-07-23	Falk, Rainer et al.	
	122	8520589		2013-08-27	Bhatt, Yogesh et al.	
	123	6542992		2003-04-01	Peirce, Kenneth L. et al.	
	124	8379847		2013-02-19	Bell, Robert H. et al.	
	125	8185093		2012-05-22	Jheng, Yu-Syuan et al.	
	126	8296404		2012-10-23	McDysan, Dave et al.	
	127	8195163		2012-06-05	Gisby, Doug et al.	
	128	8437734		2013-05-07	Ray, Amar N. et al.	
	129	8280351		2012-10-02	Ahmed, Shahid et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	130	7460837		2008-12-02	Diener, Neil R.	
	131	7653394		2010-01-26	McMillin, Brian K.	
	132	8130793		2012-03-06	Edwards, Stephen K. et al.	
	133	8509082		2013-08-13	Heinz, John M. et al.	
	134	8526329		2013-09-03	Mahany, Ronald L. et al.	
	135	5983270		1999-11-09	Abraham, Dalen M. et al.	
	136	6598034		2003-07-22	Kloth, Axel K.	
	137	7032072		2006-04-18	Quinn, Michael J. et al.	
	138	7580356		2009-08-25	Mishra, Sanjeev K. et al.	
	139	7742406		2010-06-22	Muppala, Suresh	
	140	7953877		2011-05-31	Vemula, Narendra et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	141	7957381		2011-06-07	Clermidy, Fabien et al.	
	142	8031601		2011-10-04	Feroz, Azeem et al.	
	143	8255534		2012-08-28	Assadzadeh, Alireza	
	144	8489720		2013-07-16	Morford, Michael Robert et al.	
	145	7774323		2010-08-10	Helfman, Nadav	
	146	7043268		2006-05-09	Yukie, Satoru et al.	
	147	8391262		2013-03-05	Maki, Lasse et al.	
	148	7113780		2006-09-26	McKenna, Daniel Bernard et al.	
	149	8166554		2012-04-24	John, Pramod	
	150	7697540		2010-04-13	Haddad, Reda et al.	
	151	6748195		2004-06-08	Phillips, W. Garland	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	152	8583499		2013-11-12	De Judicibus, Dario et al.	
	153	8352360		2013-01-08	De Judicibus, Dario et al.	
	154	8463232		2013-06-11	Tuli, Amol et al.	
	155	7958029		2011-06-07	Bobich, Thomas et al.	
	156	7540408		2009-06-02	Levine, Judah Joseph et al.	
	157	7826427		2010-11-02	Sood, Kapil et al.	
	158	8185088		2012-05-22	Klein, Robert S. et al.	
	159	8548428		2013-10-01	Raleigh, Gregory G.	
	160	8483694		2013-07-09	Lewis, Allan D. et al.	
	161	8351592		2013-01-08	Freeny, Jr., Charles C. et al.	
	162	8452858		2013-05-28	Wu, John et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	163	7610396		2009-10-27	Taglienti, Claudio et al.	
	164	7984511		2011-07-19	Kocher, Paul Carl et al.	
	165	7987510		2011-07-26	Kocher, Paul C. et al.	
	166	8571993		2013-10-29	Kocher, Paul C. et al.	
	167	8543265		2013-09-24	Ekhaguere, David E. et al.	
	168	8385975		2013-02-26	Forutanpour, Babak	
	169	6873988		2005-03-29	Hermann, Conrad K. et al.	
	170	7013469		2006-03-14	Smith, Adam W. et al.	
	171	7203169		2007-04-10	Okholm, Jon Eric et al.	
	172	7286834		2007-10-23	Walter, Edward	
	173	7555757		2009-06-30	Smith, Adam W. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	174	7574509		2009-08-11	Nixon, Mark J. et al.	
	175	7826607		2010-11-02	de Carvalho Resende, Mauricio Guilherme et al.	
	176	7940685		2011-05-10	Breslau, Lee Michel et al.	
	177	8196199		2012-06-05	Hrastar, Scott E. et al.	
	178	8204505		2012-06-19	Jin, Haipeng et al.	
	179	8228818		2012-07-24	Chase, Christopher J. et al.	
	180	8320244		2012-11-27	Muqattash, Alaa et al.	
	181	8411691		2013-04-02	Aggarwal, Rahul	
	182	8461958		2013-06-11	Saenz, Jorge E. et al.	
	183	8484327		2013-07-09	Werner, Eran et al.	
	184	8522039		2013-08-27	Hyndman, Arn et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	185	8544105		2013-09-24	Mclean, Ivan H. et al.	
	186	8571474		2013-10-29	Chavez, Timothy R. et al.	
	187	8194572		2012-06-05	Horvath, Robert et al.	
	188	8516552		2013-08-20	Raleigh, Gregory G.	
	189	8441955		2013-05-14	Wilkinson, Robert Todd et al.	
	190	5774532		1998-06-30	Gottlieb, Louis G. et al.	
	191	8095124		2012-01-10	Balia, Hinal K.	
	192	7797060		2010-09-14	Grgic, Richard J. et al.	
	193	7930327		2011-04-19	Craft, David Jones et al.	
	194	8264965		2012-09-11	Dolganow, Andrew et a.	
	195	8626115		2014-01-07	Raleigh, Gregory G. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	196	6885997		2005-04-26	Roberts, David T.	
	197	8229394		2012-07-24	Karlberg, Johan	
	198	8495700		2013-07-23	Shahbazi, Majid	
	199	8548427		2013-10-01	Chow, Paulo S.T. et al.	
	200	8572117		2013-10-29	Rappaport, Theodore S.	
	201	8589955		2013-11-19	Roundtree, Brian et al.	
	202	8660853		2014-02-25	Robb, Terence A. et al.	
	203	8601125		2013-12-03	Huang, Shibi et al	
	204	8046449		2011-10-25	Yoshiuchi, Hideya	
	205	8635164		2014-01-21	Rosenhaft, Matthew et al.	
	206	8566236		2013-10-22	Busch, James David	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	207	8528068		2013-09-03	Weglein, Joseph et al.	
	208	8442015		2013-05-14	Behzad, Arya et al	
	209	7853255		2010-12-14	Karaoguz, Jeyhan et al	
	210	7720464		2010-05-18	Batta, Puneet	
	211	8300575		2012-10-30	Willars, Per	
	212	8666395		2014-03-04	Silver, Andrew	
	213	8315593		2012-11-20	Gallant, John K. et al.	
	214	8180881		2012-05-15	Seo, Kyoung-Il et al.	
	215	7539132		2009-05-26	Werner, Carl E. et al.	
	216	8589541		2013-11-19	Raleigh, Gregory G. et al.	
	217	7805606		2010-09-28	Birger, Chet et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	218	8347378		2013-01-01	Merkin, Aaron E. et al.	
	219	8391834		2013-03-05	Raleigh, Gregory G.	
	220	6185576		2001-02-06	McIntosh, Lowrie	
	221	8175574		2012-05-08	Panda, Biswaranjan et al.	
	222	8375128		2013-02-12	Tofighbakhsh, Mostafa et al.	
	223	8527410		2013-09-03	Markki, Outi et al.	
	224	7320029		2008-01-15	Rinne, Janne Petri et al.	
	225	8275415		2012-09-25	Huslak, Nicholas S.	
	226	8539561		2013-09-17	Gupta, Akhilesh et al.	
	227	8554876		2013-10-08	Winsor, Gerald W.	
	228	8191124		2012-05-29	Wynn, Simon et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	229	7805140		2010-09-28	Friday, Robert J. et al.	
	230	8605691		2013-12-10	Soomro, Amjad et al.	
	231	8655357		2014-02-18	Gazzard, Daryl Robert et al.	
	232	8706863		2014-04-22	Fadell, Anthony	
	233	6640334		2003-10-28	Rasmussen, John H.	
	234	7668612		2010-02-23	Okkonen, Harri	
	235	5325532		1994-06-28	Crosswy, Wm. Caldwell et al.	
	236	7614051		2009-11-03	Glaum, Jeffrey D. et al.	
	237	5131020		1992-07-14	Liebesny, John P. et al.	
	238	8223741		2012-07-17	Bartlett, Roger Danforth et al.	
	239	8396458		2013-03-12	Raleigh, Gregory G.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	240	8370483		2013-02-05	Choong et al.	
	241	8670334		2014-03-11	Keohane et al.	
	242	8693323		2014-04-08	McDysan, David E.	
	243	7409447		2008-08-05	Assadzadeh, Alireza	
	244	8725899		2014-05-13	Short, Joel et al.	
	245	8676925		2014-03-18	Liu, Jiawei et al.	
	246	8645518		2014-02-04	David, Scott L.	
	247	7756056		2010-07-13	Kim et al	
	248	8131281		2012-03-06	Hildner et al.	
	249	8160598		2012-04-17	Savoor, Raghvendra	
	250	8375136		2013-02-12	Roman et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	251	6119933		2000-09-19	Wong et al.	
	252	8694772		2014-04-08	Kao et al.	
	253	8719423		2014-05-06	Wyld, Jeremy	
	254	8347104		2013-01-01	Pathiyal, Krishna K.	
	255	7149229		2006-12-12	Leung, Kent K.	
	256	7242668		2007-07-10	Kan, Chao et al.	
	257	8095640		2012-01-10	Guingo, Pierrick et al.	
	258	8705361		2014-04-22	Venkataraman, Ramesh et al.	
	259	8780857		2014-07-15	Balasubramanian, Srinivasan et al.	
	260	8811991		2014-08-19	Jain, Nikhil et al.	
	261	7809351		2010-10-05	Panda et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	262	8346210		2013-01-01	Balsan, Damien et al.	
	263	8355696		2013-01-15	Olding et al.	
	264	8488597		2013-07-16	Nie et al.	
	265	6438575		2002-08-20	Khan et al.	
	266	7222304		2007-05-22	Beaton et al.	
	267	7561899		2009-07-14	Lee, Changseok	
	268	8200200		2012-06-12	Belser et al.	
	269	8229914		2012-07-24	Ramer et al.	
	270	8522249		2013-08-27	Beaule, Stephane	
	271	8701015		2014-04-15	Bonnat, Pierre	
	272	6697821		2004-02-24	Ziff et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	273	6763226		2004-07-13	McZeal Jr., Alfred	
	274	6982733		2006-01-03	McNally et al.	
	275	6983370		2006-01-03	Eaton, et al.	
	276	7318111		2008-01-08	Zhao, Wen	
	277	8064418		2011-11-22	Maki, Lasse	
	278	8249601		2012-08-21	Emberson et al.	
	279	8514927		2013-08-20	Sundararajan et al.	
	280	8634425		2014-01-21	Gorti et al.	
	281	8825109		2014-09-02	Montemurro et al.	
	282	9014973		2015-04-21	Ruckart, John	
	283	8977284		2015-03-10	Reed, Mark J.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	284	8930238		2015-01-06	Coffman et al.	
	285	8880047		2014-11-04	Konicek et al.	
	286	8739035		2014-05-27	Trethewey, Jim	
	287	8571598		2013-07-16	Valavi, John J.	
	288	8489110		2013-07-16	Frank et al.	
	289	8406736		2013-03-26	Das et al.	
	290	8259692		2012-09-04	Bajko, Gabor	
	291	8233433		2012-07-31	Kalhan, Amit	
	292	8155666		2012-04-10	Alizadeh-Shabdiz, Farshid	
	293	8103285		2012-01-24	Kalhan, Amit	
	294	7936736		2011-05-03	Proctor Jr., James Arthur et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	295	7925778		2011-04-12	Wijnands et al.	
	296	7760137		2010-07-20	Martucci et al.	
	297	7684370		2010-03-23	Kezys, Vytautas Robertas	
	298	7084775		2006-08-01	Smith, Michael R.	
	299	6578076		2003-06-10	Putzolu, David Matthew	
	300	7133695		2006-11-07	Beyda, William J.	

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]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	1	1538730A	CN		2004-10-20	Zhongxing Communication Co., Ltd.		
	2	101115248A	CN		2008-01-30	Lenovo Beijing Ltd.		
	3	101341764A	CN		2009-01-07	Telefonaktiebolaget LM Ericsson		
	4	2007068288A1	WO		2007-06-21	Telefonaktiebolaget LM Ericsson		
	5	1802839A	CN		2006-07-12	Motorola Inc.		
	6	2004064306A2	WO		2004-07-29	Motorola Inc.		
	7	101123553A	CN		2007-09-11	SouTheast University		
	8	1937511A	CN		2007-03-28	ZTE		
	9	2466831A1	EP		2012-06-20	Openet Telecom Ltd./ McNamee et al.		
	10	1999027723 A1	WO		1999-06-03	Telefonaktiebolaget LM Ericsson		
	11	2007133844	WO		2007-11-22	Camiant, Inc.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	12	2011149532 A1	WO		2011-12-01	Raleigh, Gregory G. et al.		
	13	101183958A	CN		2008-05-21	Huawei Tech. Co. Ltd.		
	14	1801829A	CN		2006-07-12	Kunda Computer Technology (Kunshan) Co., Ltd.		
	15	1867024A	CN		2006-11-22	Huawei Technologies Co., Ltd.		
	16	101815275A	CN		2010-08-25	Yang, Liu		

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.	T5
	1	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	
	2	"The Construction of Intelligent Residential District in Use of Cable Television Network," Shandong Science, Vol. 13, No. 2, June 2000	
	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	"Prevent iCloud Documents & Data from using your data plan," October 26, 2011; CNET webarchive, by Jason Ciprian	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	5	'3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 11)," 3GPP Standard; 3GPP TS 23.203 v11.6.0; Sophia Antipolis, France; pp. 1-177; June 2012	
	6	'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	
	7	'ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	10/10/2017

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	5577100		1996-11-19	McGREGOR et al.	
	2	5794142		1998-08-11	VANTTILA et al.	
	3	5892900		1999-04-06	GINTER et al.	
	4	5903845		1999-05-11	BUHRMANN et al.	
	5	5933778		1999-08-03	BUHRMANN et al.	
	6	5940472		1999-08-17	NEWMAN et al.	
	7	6047268		2000-04-04	BARTOLI et al.	
	8	6078953		2000-06-20	VAID et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	9	6098878		2000-08-08	DENT et al.	
	10	6141686		2000-10-31	JACKOWSKI et al.	
	11	6148336		2000-11-14	THOMAS et al.	
	12	6198915		2001-03-06	McGREGOR et al.	
	13	6263055		2001-07-17	GARLAND et al.	
	14	6317584		2001-11-13	ABU-AMARA et al.	
	15	6418147		2002-07-09	WIEDEMAN, Robert A.	
	16	6449479		2002-09-10	SANCHEZ, Eduardo	
	17	6532235		2003-03-11	BENSON et al.	
	18	6532579		2003-03-11	SATO et al.	
	19	6539082		2003-03-25	LOWE et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	20	6563806		2003-05-13	YANO et al.	
	21	6574321		2003-06-03	COX et al.	
	22	6574465		2003-06-03	MARSH et al.	
	23	6603969		2003-08-05	VUORISTO et al.	
	24	6639975		2003-10-28	O'NEAL et al.	
	25	6650887		2003-11-18	McGREGOR et al.	
	26	6651101		2003-11-18	GAI et al.	
	27	6658254		2003-12-02	PURDY et al.	
	28	6684244		2004-01-27	GOLDMAN et al.	
	29	6725031		2004-04-20	WATLER et al.	
	30	6765864		2004-07-20	NATARAJAN et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	31	6785889		2004-08-31	WILLIAMS, Peter	
	32	6829596		2004-12-07	FRAZEE, Steve	
	33	6829696		2004-12-07	BALMER et al.	
	34	6920455		2005-07-19	WESCHLER, Paul	
	35	6952428		2005-10-04	NECKA et al.	
	36	6965667		2005-11-15	TRABANDT et al.	
	37	6996076		2006-02-07	FORBES et al.	
	38	6998985		2006-02-14	REISMAN et al.	
	39	7024200		2006-04-04	McKENNA et al.	
	40	7027408		2006-04-11	NABKEL et al.	
	41	7042988		2006-05-09	JUITT et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	42	7058968		2006-06-06	ROWLAND et al.	
	43	7069248		2006-06-27	HUBER, Adriano	
	44	7092696		2006-08-15	HOSAIN et al.	
	45	7142876		2006-11-28	TROSSEN et al.	
	46	7158792		2007-01-02	COOK et al.	
	47	7174174		2007-02-06	BORIS et al.	
	48	7180855		2007-02-20	LIN , Wei	
	49	7197321		2007-03-27	ERSKINE et al.	
	50	7242920		2007-07-10	MORRIS, Robert P.	
	51	7245901		2007-07-17	McGREGOR et al.	
	52	7280816		2007-10-09	FRATTI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	53	7280818		2007-10-09	CLAYTON, Steve	
	54	7289489		2007-10-30	KUNG et al.	
	55	7290283		2007-10-30	COPELAND III, John A.	
	56	7317699		2008-01-08	GODFREY et al.	
	57	7322044		2008-01-22	HRASTAR, Scott E.	
	58	7324447		2008-01-29	MORFORD, Michael Robert	
	59	7325037		2008-01-29	LAWSON, Karen L.	
	60	7349695		2008-03-25	OOMMEN et al.	
	61	7353533		2008-04-01	WRIGHT et al.	
	62	7356337		2008-04-08	FLORENCE, Shahar	
	63	7366497		2008-04-29	NAGATA, Hideaki	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	64	7373136		2008-05-13	WATLER et al.	
	65	7388950		2008-06-17	ELSEY et al.	
	66	7401338		2008-07-15	BOWEN et al.	
	67	7403763		2008-07-22	MAES, Stephane H.	
	68	7418253		2008-08-26	KAVANAH, Alan	
	69	7421004		2008-09-02	FEHER, Kamilo	
	70	7450591		2008-11-11	KORLING et al.	
	71	7450927		2008-11-11	CRESWELL et al.	
	72	7486185		2009-02-03	CULPEPPER et al.	
	73	7499537		2009-03-03	ELSEY et al.	
	74	7516219		2009-04-07	MOGHADDAM et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	75	7574731		2009-08-11	FASCENDA, Anthony C.	
	76	7580857		2009-08-25	VanFLEET et al.	
	77	7610328		2009-10-27	HAASE et al.	
	78	7617516		2009-11-10	HUSLAK et al.	
	79	7620065		2009-11-17	FALARDEAU, Eric	
	80	7620162		2009-11-17	AARON et al.	
	81	7647047		2010-01-12	MOGHADDAM et al.	
	82	7650137		2010-01-19	JOBS et al.	
	83	7668903		2010-02-23	EDWARDS et al.	
	84	7693720		2010-04-06	KENNEWICK et al.	
	85	7720505		2010-05-18	GOPI et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	86	7734784		2010-06-08	ARAUJO et al.	
	87	7747240		2010-06-29	BRISCOE et al.	
	88	7747699		2010-06-29	PRUEITT et al.	
	89	7792708		2010-09-07	ALVA, Jessi	
	90	7797204		2010-09-14	BALENT, Bruce F.	
	91	7797401		2010-09-14	STEWART et al.	
	92	7822837		2010-10-26	URBAN et al.	
	93	7848768		2010-12-07	OMORI et al.	
	94	7868778		2011-01-11	KENWRIGHT, David Norris	
	95	7873705		2011-01-18	KALISH, Dan	
	96	7882029		2011-02-01	WHITE, Craig R.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	97	7929960		2011-04-19	MARTIN et al.	
	98	7937069		2011-05-03	RASSAM, Frederic	
	99	7941184		2011-05-10	PRENDERGAST et al.	
	100	7949529		2011-05-24	WEIDER et al.	
	101	7957511		2011-06-07	DRUDIS et al.	
	102	7975184		2011-07-05	GOFF et al.	
	103	7984130		2011-07-19	BOGINENI et al.	
	104	7986935		2011-07-26	D'SOUZA et al.	
	105	8005459		2011-08-23	BALSILLIE, Jim	
	106	8010080		2011-08-30	THENTHIRUPERAI et al.	
	107	8010081		2011-08-30	ROSKOWSKI, Steve	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	108	8015133		2011-09-06	WU et al.	
	109	8015234		2011-09-06	LUM et al.	
	110	8019687		2011-09-13	WANG et al.	
	111	8023425		2011-09-20	RALEIGH, Gregory G.	
	112	8095666		2012-01-10	SCHMIDT et al.	
	113	8099077		2012-01-17	CHOWDHURY et al.	
	114	8099517		2012-01-17	JIA et al.	
	115	8144591		2012-03-27	GHAI et al.	
	116	8170553		2012-05-01	BENNETT, James D.	
	117	6606744		2003-08-12	MIKURAK, Michael G.	
	118	7336960		2008-02-26	ZAVALKOVSKY et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	119	8190675		2012-05-29	TRIBBETT, David	
	120	8194549		2012-06-05	HUBER et al.	
	121	8200775		2012-06-12	MOORE, James F.	
	122	8135392		2012-03-13	MARCELLINO et al.	
	123	7953808		2011-05-31	SHARP et al.	
	124	6502131		2002-12-31	VAID, Aseem et al.	
	125	6505114		2003-01-07	LUCIANI, Sergio	
	126	6763000		2004-07-13	WALSH, Peter J.	
	127	6967958		2005-11-22	ONO, Yoshiyuki et al.	
	128	7644267		2010-01-05	YLIKOSKI, Martti et al.	
	129	7710932		2010-05-04	MUTHUSWAMY, Sivakumar et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	130	7881199		2011-02-01	KRSTULICH, Zlatko	
	131	7886047		2011-02-08	POTLURI, Dora	
	132	7911975		2011-03-22	DROZ, Patrick et al.	
	133	8050275		2011-11-01	IYER, Jayaraman R.	
	134	8194553		2012-06-05	LIANG, Zhi Yong et al.	
	135	8239520		2012-08-07	GRAH, Adrian	
	136	7890084		2011-02-15	Dudziak, Thaddeus Jude et al.	
	137	7890111		2011-02-15	Bugenhagen, Michael K.	
	138	6226277		2001-05-01	Chuah, Mooi Choo	
	139	6839340		2005-01-04	Voit, Eric A. et al.	
	140	6922562		2005-07-26	Ward, Stephen L. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	141	7620041		2009-11-17	Dunn, Jeffrey H. et al.	
	142	7627314		2009-12-01	Carlson, Steven I. et al.	
	143	7792538		2010-09-07	Kozisek, Steven E.	
	144	7801523		2010-09-21	Kenderov, Stoyan	
	145	7877090		2011-01-25	Maes, Stephane H.	
	146	7912025		2011-03-22	Pattenden, Christopher E. S. et al.	
	147	7948968		2011-05-24	Voit, Eric A. et al.	
	148	7970426		2011-06-28	Poe, Brian R. et al.	
	149	8185158		2012-05-22	Tamura, Motoshi et al.	
	150	8254915		2012-08-28	Kozisek, Steven E.	
	151	7418257		2008-08-26	Kim, Myong-Ju	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	152	8126123		2012-02-28	Cai, Yigang et al.	
	153	7903553		2011-03-08	Liu, Enhui	
	154	8155620		2012-04-10	Wang, Jun et al.	
	155	8238287		2012-08-07	Gopi, Paramesh et al.	
	156	7113997		2006-09-26	Jayapalan, Jay et al.	
	157	5594777		1997-01-14	Makkonen, Matti et al.	
	158	8244241		2012-08-14	Montemurro, Michael	
	159	7756534		2010-07-13	Anupam, Vinod et al.	
	160	7636574		2009-12-22	Poosala, Viswanath	
	161	6678516		2004-01-13	Nordman, Ian et al.	
	162	6477670		2002-11-05	Ahmadvand, Nima	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	163	6038452		2000-03-14	Strawczynski, Leo et al.	
	164	8108520		2012-01-31	Ruutu, Jussi et al.	
	165	7778643		2010-08-17	Laroia, Rajiv et al.	
	166	7668176		2010-02-23	Chuah, Mooi Choo	
	167	7515608		2009-04-07	Yuan, Yuan et al.	
	168	7251218		2007-07-31	Jorgensen, Jacob W.	
	169	7002920		2006-02-21	Ayyagari, Deepak et al.	
	170	7685131		2010-03-23	Batra, Vishal Singh et al.	
	171	7283561		2007-10-16	Picher-Dempsey, Heidi	
	172	7212491		2007-05-01	Koga, Takahiro	
	173	6683853		2004-01-27	Kannas, Chris et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	174	8064896		2011-11-22	BELL, Kris M. et al.	
	175	8160015		2012-04-17	RASHID, Mohammed H. et al.	
	176	8275830		2012-09-25	Raleigh, Gregory G.	
	177	7609700		2009-10-27	Ying, Wen-Ping et al.	
	178	8255515		2012-08-28	MELMAN, David et al.	
	179	7945240		2011-05-17	KLOCK, Jacqueline et al.	
	180	7912056		2011-03-22	BRASSEM, Wayne	
	181	7920529		2011-04-05	MAHLER, Roger et al.	
	182	8184530		2012-05-22	SWAN, Tim L. et al.	
	183	8214536		2012-07-03	ZHAO, Wen	
	184	8213363		2012-07-03	Ying, Wen-Ping et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	185	8255689		2012-08-28	KIM, Eun Ah et al.	
	186	7746854		2010-06-29	AMBE, Shekhar et al.	
	187	7068600		2006-06-27	CAIN, Joseph Bibb	
	188	6876653		2005-04-05	AMBE, Shekhar et al.	
	189	6631122		2003-10-07	ARUNACHALAM, Vaidhyanathan et al.	
	190	7599288		2009-10-06	COLE, Raymond E. et al.	
	191	7546629		2009-06-09	ALBERT, Anthony et al.	
	192	7747730		2010-06-29	HARLOW, James D.	
	193	7609650		2009-10-27	ROSKOWSKI, Steve et al.	
	194	6581092		2003-06-17	MOTOYAMA, Tetsuro	
	195	7283963		2007-10-16	FITZPATRICK, John E. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	196	8271049		2012-09-18	SILVER, Andrew et al.	
	197	7644151		2010-01-05	JERRIM, John et al.	
	198	8291238		2012-10-16	GINTER, Karl L. et al.	
	199	8068824		2011-11-29	SHAN, Xueshan et al.	
	200	7228354		2007-06-05	CHAMBLISS, David Darden et al.	
	201	5283904		1994-02-01	CARSON, David G. et al.	
	202	8208919		2012-06-26	KOTECHA, Lalit Ratilal	
	203	8185152		2012-05-22	GOLDNER, Alla	
	204	7844728		2010-11-30	ANDERSON, Thomas W. et al.	
	205	7873344		2011-01-18	BOWSER, Robert et al.	
	206	7856226		2010-12-21	WONG, Ellis L. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	207	7948952		2011-05-24	HURTTA, Tuija et al.	
	208	7957020		2011-06-07	MINE, Ryuta et al.	
	209	7346410		2008-03-18	UCHIYAMA, Kenji	
	210	7167078		2007-01-23	POURCHOT, Shawn C.	
	211	8102814		2012-01-24	RAHMAN, Shahriar I. et al.	
	212	7970350		2011-06-28	SHEYNMAN, Arnold	
	213	8094551		2012-01-10	HUBER, Kurt Donald et al.	
	214	8335161		2012-12-18	Foottit, Tom et al.	
	215	8315594		2012-11-20	Mauser, Edward Ronald et al.	
	216	8135388		2012-03-13	Gailloux, Michael A. et al.	
	217	6947723		2005-09-20	Gurnani, Roger et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	218	8353001		2013-01-08	Herrod, Allan	
	219	8195093		2013-06-05	Garrett, Darrin et al.	
	220	8036600		2011-10-11	Garrett, Darrin et al.	
	221	8301513		2012-10-30	Peng, Shih-Ta et al.	
	222	8230061		2012-07-24	Hassan, Amer A. et al.	
	223	8204794		2012-06-19	Peng, Shih-Ta et al.	
	224	8350700		2013-01-08	Fast, Raymond D. et al.	
	225	8204190		2012-06-19	Bang, Jung-Hee et al.	
	226	7865182		2011-01-04	Macaluso, Anthony G.	
	227	7962622		2011-06-14	Friend, John et al.	
	228	7583964		2009-09-01	Wong, Gregory A.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	229	7565141		2009-07-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	240	7711848		2010-05-04	MAES, Stephane H.	
	241	6782412		2004-08-24	BROPHY, Kevin et al.	
	242	6081591		2000-06-27	SKOOG, Frederick H.	
	243	6064878		2000-05-16	DENKER, John Stewart et al.	
	244	7730123		2010-06-01	ERICKSON, Richard R. et al.	
	245	8024397		2011-09-20	ERICKSON, Richard R. et al.	
	246	8156206		2012-04-10	KILEY, Kevin J. et al.	
	247	8126722		2012-02-28	ROBB, Terence Alan et al.	
	248	8364089		2013-01-29	PHILLIPS, Derek	
	249	6754470		2004-06-22	Hendrickson, Keith et al.	
	250	8122128		2012-02-21	Burke, II, Robert M. et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	251	8149823		2012-04-03	Turcan, Diane Brown et al.	
	252	8326359		2012-12-04	Kauffman, Donald C.	
	253	8131256		2012-03-06	MARTTI, Jyrki et al.	
	254	6381316		2002-04-30	JOYCE, Simon James et al.	
	255	7965983		2011-06-21	SWAN, Tim et al.	
	256	8284740		2012-10-09	O'CONNOR, Dennis M.	
	257	8116223		2012-02-14	TIAN, Dan et al.	
	258	6154738		2000-11-28	CALL, Charles Gainor	
	259	8423016		2013-04-16	BUCKLEY, Adrian et al.	
	260	8306518		2012-11-06	GAILLOUX, Michael A.	
	261	8422988		2013-04-16	KESHAV, Srinivasan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	262	6035281		2000-03-07	Crosskey, James P. et al.	
	263	6996393		2006-02-07	Pyhalammi, Seppo et al.	
	264	7760711		2010-07-20	Kung, Fen-Chung et al.	
	265	8000318		2011-08-16	Wiley, William L. et al.	
	266	8098579		2012-01-17	Ray, Amar N. et al.	
	267	8155670		2012-04-10	Fullam, Scott et al.	
	268	8374090		2013-02-12	Morrill, Robert J. et al.	
	269	7457265		2008-11-25	Julka, Vibhor et al.	
	270	7729326		2010-06-01	Sekhar, Ramesh	
	271	7929973		2011-04-19	Zavalkovsky, Arthur et al.	
	272	7945945		2011-05-17	Graham, Richard et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	273	8059530		2011-11-15	Cole, Terry L.	
	274	8266681		2012-09-11	Deshpande, Sumit B. et al.	
	275	8280354		2012-10-02	Smith, Christopher et al.	
	276	8331293		2012-12-11	Sood, Kapil	
	277	8019820		2011-09-13	Son, Giyeong et al.	
	278	8191116		2012-05-29	Gazzard, Daryl	
	279	6292828		2001-09-18	Williams, David L.	
	280	7043226		2006-05-09	Yamauchi, Toshiaki	
	281	7472189		2008-12-30	Mallya, Arvind R. et al.	
	282	7944948		2011-05-17	Chow, Albert T. et al.	
	283	7802724		2010-09-28	Nohr, Steven Paul	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	284	8155155		2012-04-10	Chow, Albert T. et al.	
	285	8447324		2013-05-21	Shuman, Mohammed Ataur et al.	
	286	8005009		2011-08-23	McKee, Neil et al.	
	287	7760861		2010-07-20	Croak, Marian et al.	
	288	8060463		2011-11-15	Spiegel, Joel R.	
	289	8224773		2012-07-17	Spiegel, Joel R.	
	290	8352980		2013-01-08	Howcroft, Jerald Robert	
	291	8386386		2013-02-26	Zhu, Kevin	
	292	8347362		2013-01-01	Cai, Yigang et al.	
	293	8340718		2012-12-25	Colonna, Massimo et al.	
	294	8385896		2013-02-26	Proctor Jr., James A. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	295	8320949		2012-11-27	Matta, Sudheer Poorna Chandra	
	296	8279864		2012-10-02	Wood, Daniel M.	
	297	8271045		2012-09-18	Parolkar, Satish et al.	
	298	8233883		2012-07-31	De Froment, Eric	
	299	8224382		2012-07-17	Bultman, Michael J.	
	300	8184590		2012-05-22	Rosenblatt, Ariel	

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]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	1	1463238	EP		2004-09-29	Alcatel		
	2	1739518	EP		2007-01-03	Research In Motion Limited		
	3	1772988	EP		2007-04-11	Huawei Technologies Co., Ltd.		
	4	1978772	EP		2008-10-08	British Telecommunications Public Limited Company		
	5	1999065185	WO		1999-12-16	British Telecommunications Public Limited Company		
	6	2003014891	WO		2003-02-20	The Boeing Company		
	7	2003058880	WO		2003-07-17	Telia AB		
	8	2004028070	WO		2004-04-01	Credant Technologies, Inc.		
	9	2004077797	WO		2004-09-10	Boston Communications Group, Inc. (Erskine)		
	10	2004095753	WO		2004-11-04	Motorola Inc.		
	11	2006004467	WO		2006-01-12	Telefonaktiebolaget LM Ericsson		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	12	2006050758	WO		2006-05-18	Telefonaktiebolaget LM Ericsson		
	13	2006073837	WO		2006-07-13	Symbol Technologies, Inc.		
	14	2006077481	WO		2006-07-27	TrueContext Corporation		
	15	2006130960	WO		2006-12-14	Mobidia, Inc.		
	16	2007001833	WO		2007-01-04	Symbol Technologies, Inc.		
	17	2007014630	WO		2007-02-08	Telefonaktiebolaget LM Ericsson		
	18	2007018363	WO		2007-02-15	Upresto, Inc.		
	19	2007053848	WO		2007-05-10	Mobile Armor, LLC		
	20	2007069245	WO		2007-06-21	Yoggie Security Systems, Inc.		
	21	2007107701	WO		2007-09-27	British Telecommunications Public Limited Company		
	22	2008017837	WO		2008-02-14	Symbian Software Limited		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	23	2008051379	WO		2008-05-02	Verizon Services Corp.		
	24	2008066419	WO		2008-06-05	Telefonaktiebolaget LM Ericsson		
	25	2008080139	WO		2008-07-03	Integrated Mobile, Inc.		
	26	2008080430	WO		2008-07-10	Telecom Italia S.P.A.		
	27	2008099802	WO		2008-08-21	NEC Corporation		
	28	2010088413	WO		2010-08-05	Headwater Partners I LLC		
	29	2006120558	WO		2006-11-16	Nokia Corp.		
	30	1889777A	CN		2006-07-19	Huawei Tech. Co. Ltd.		
	31	101155343A	CN		2006-09-29	Huawei Tech. Co. Ltd.		
	32	101035308A	CN		2006-03-09	Huawei Tech. Co. Ltd.		
	33	2007124279	WO		2007-11-01	Cisco Technology, Inc., et al.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	34	2005008995	WO		2005-01-27	Starhub Ltd.		
	35	1998058505	WO		1998-12-23	Sonera Oy		
	36	2007097786	WO		2007-08-30	Sony Ericsson Mobile Communications AB		

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.	T5
	1	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	
	2	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	
	3	ALONISTIOTI et al., "Intelligent Architectures Enabling Flexible Service Provision and Adaptability," 2002	
	4	Amazon Technologies, Inc., "Kindle™ User's Guide," 3rd Edition, Copyright 2004-2009	
	5	CHANDRASEKHAR et al., "Femtocell Networks: A Survey," June 28, 2008	
	6	CHAOUCHI et al., "Policy Based Networking in the Integration Effort of 4G Networks and Services," 2004 IEEE	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	7	Cisco Systems, Inc., "Cisco Mobile Exchange (CMX) Solution Guide: Chapter 2 - Overview of GSM, GPRS, and UMTS," November 4, 2008	
	8	DIKAIAKOS et al., "A Distributed Middleware Infrastructure for Personalized Services," November 24, 2003	
	9	European Commission, "Data Roaming Tariffs - Transparency Measures," [online] retrieved from http://web.archive.org/web/20081220232754/http://ec.europa.eu/information_society/activities/roaming/data/measures/index_en.htm, December 20, 2008 [retrieved May 16, 2012]	
	10	FAROOQ et al., "An IEEE 802.16 WiMax Module for the NS-3 Simulator," March 2-6, 2009	
	11	HAN et al., "Information Collection Services for Qos-Aware Mobile Applications," 2005	
	12	HARTMANN et al., "Agent-Based Banking Transactions & Information Retrieval - What About Performance Issues?" 1999	
	13	Hewlett-Packard Development Company, LP, "IP Multimedia Services Charging," white paper, January 2006	
	14	HOSSAIN et al., "Gain-Based Selection of Ambient Media Services in Pervasive Environments," Mobile Networks and Applications. 03 October 2008	
	15	KNIGHT et al., "Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standarization Efforts," IEEE Communications Magazine, June 2004	
	16	KOUTSOPOULOU et al., "Middleware Platform for the Support of Charging Reconfiguration Actions," 2005	
	17	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	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	18	LI, Yu, "Dedicated E-Reading Device: The State of the Art and The Challenges," Scroll, Vol. 1, No. 1, 2008	
	19	NILSSON et al., "A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA," February 2006	
	20	OPPLIGER, Rolf, "Internet Security: Firewalls and Bey," Communications of the ACM, May 1997, Vol. 40. No. 5	
	21	RAO et al., "Evolution of Mobile Location-Based Services," Communication of the ACM, December 2003	
	22	STEGLICH, Stephan, "I-Centric User Interaction," November 21, 2003	
	23	VAN EIJK, et al., "GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage," July 1, 2002	
	24	ZHU et al., "A Survey of Quality of Service in IEEE 802.11 Networks," IEEE Wireless Communications, August 2004	
	25	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)	
	26	Ruckus Wireless – White Paper; "Smarter Wi-Fi for Mobile Operator Infrastructures" 2010	
	27	Accuris Networks, "The Business Value of Mobile Data Offload – a White Paper", 2010	
	28	Wireless Broadband Alliance, "WISPr 2.0, 08 April, 2010"; Doc. Ref. No.: WBA/RM/WISPr, Version 01.00	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	29	THURSTON, Richard, "WISPr 2.0 Boosts Roaming Between 3G and Wi-Fi"; June 23, 2010; Web page from zdnet.com; Zdnet.com/wispr-2-0-boosts-roaming-between-3g-and-wi-fi-3040089325/	
	30	Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group, "Hotspot 2.0 (Release 1) Technical Specification – Version 1.0.0"; 2012	
	31	Wi-Fi Alliance Hotspot 2.0 Technical Task Group, "Wi-Fi Certified Passpoint™ (Release 1) Deployment Guidelines – Version 1.0 – October 2012"	

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	10/10/2017

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination	
	15/287,597	RALEIGH ET AL.	
	Examiner	Art Unit	
	ANDREW JOSEPH RUDY	3687	

SEARCHED			
Class	Subclass	Date	Examiner
705	300	10/12/2017	AJR
G06Q	10/101	10/12/2017	AJR
G06Q	10/10	10/12/2017	AJR
G06Q	30/04	10/12/2017	AJR
G06Q	30/0601	10/12/2017	AJR
G06F	17/30286	10/12/2017	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	10/12/2017	AJR
Inventor name search conducted.	10/12/2017	AJR
Bibliographic data updated.	10/12/2017	AJR

IPR2025-01572
Apple EX1002 Page 702

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Raleigh
Art Unit	2447
Examiner Name	not yet assigned
Attorney Docket Number	RALEP041D1C1

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	9137389		2015-09-15	Neal et al.	
	2	8799227		2014-08-05	Ferguson et al.	
	3	9002322		2015-04-07	Cotterill, Stephen Hayden	
	4	9361451		2016-06-07	Oberheide et al.	
	5	9369959		2016-06-14	Ruutu et al.	

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	20070259656		2007-11-08	Jeong, Jong Woo	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	2	20080263348		2008-10-23	Zaltsman, Etai et al.	
	3	20080313315		2008-12-18	Karaoguz, Jeyhan et al.	
	4	20090282127		2009-11-12	LeBlanc, Michael et al.	
	5	20100167696		2010-07-01	Smith, Christopher David et al.	
	6	20030188006		2003-10-02	Bard, Steven R.	
	7	20060160536		2006-07-20	Chou, Joey	
	8	20060168128		2006-07-27	Sistla, Amber et al.	
	9	20040203833		2004-10-14	Rathunde, Dale F. et al.	
	10	20050186948		2005-08-25	Gallagher, Michael D. et al.	
	11	20070147317		2007-06-28	Smith, Brian K. et al.	
	12	20080270212		2008-10-30	Blight, Jeffrey et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	13	20080056273		2008-03-06	Pelletier, Ghyslain et al.	
	14	20110110309		2011-05-12	Bennett, James D.	
	15	20100030890		2010-02-04	Dutta, Satadip et al.	
	16	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	
	17	20080025230		2008-01-31	Patel, Alpesh et al.	
	18	20040170191		2004-09-02	Guo, Zihua et al.	
	19	20020188732		2002-12-12	Buckman, Charles R. et al.	
	20	20080034419		2008-02-07	Mullick, Amarnath et al.	
	21	20080010379		2008-01-10	Zhao, Hang	
	22	20080139210		2008-06-12	Gisby, Doug et al.	
	23	20040243992		2004-12-02	Gustafson, James P. et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	24	20070226775		2007-09-27	Andreasen, Flemming Stig et al.	
	25	20100235329		2010-09-16	Koren, David et al	
	26	20090254857		2009-10-08	Romine, Christopher et al.	
	27	20120101952		2012-04-26	Raleigh, Gregory G. et al.	
	28	20080166993		2008-07-10	Gautier et al.	
	29	20040137890		2004-07-15	Kalke, Catherine	
	30	20070143824		2007-06-21	Shahbazi, Majid	
	31	20070266422		2007-11-15	Germano et al.	
	32	20090044185		2009-02-12	Krivopaltsev, Eugene	
	33	20040039792		2004-02-26	Nakanishi, Tomoaki	
	34	20050075115		2005-04-07	Corneille et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	35	20050239447		2005-10-27	Holzman et al.	
	36	20070213054		2007-09-13	Han, Seung-Wook	
	37	20080032715		2008-02-07	Jia et al.	
	38	20090163173		2009-06-25	Williams, Timothy D.	
	39	20100075666		2010-03-25	Garner, Neil Robert	
	40	20080293395		2008-11-27	Matthews, Ajit et al.	
	41	20050245241		2005-11-03	Durand, Terry et al.	
	42	20080125079		2008-05-29	O'Neil, Douglas et al.	
	43	20050135264		2005-06-23	Popoff, Jeff et al.	
	44	20070165630		2007-07-19	Rasanen, Jorma	
	45	20100287599		2010-11-11	HE, Xianhui	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	46	20070060200		2007-03-15	Boris et al.	
	47	20060030306		2006-02-09	Kuhn, Brian Gerald	
	48	20060035631		2006-02-16	White et al.	
	49	20060206709		2006-09-14	Labrou et al.	
	50	20090046707		2009-02-19	Smires et al.	
	51	20100311402		2010-12-09	Srinivasan et al.	
	52	20110277019		2011-11-10	Pritchard Jr., John Russell	
	53	20050250536		2005-11-10	Deng et al.	
	54	20070192460		2007-08-16	Choi et al.	
	55	20080080457		2008-04-03	Cole, Terry L.	
	56	20090049518		2009-02-19	Roman et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	57	20100248719		2010-09-30	Scholaert, Hugh	
	58	20060072451		2006-04-06	Ross, Alan D.	
	59	20070294410		2007-12-20	Pandya et al.	
	60	20070293191		2007-12-20	Mir et al.	
	61	20110145920		2011-06-16	Mahaffey et al.	
	62	20130326356		2013-12-05	Zheng et al.	
	63	20070005795		2007-01-04	Gonzalez, Ruben	
	64	20080282319		2008-11-13	Fontijn et al.	
	65	20080050715		2008-02-28	Golczewski et al.	
	66	20040259534		2004-12-23	Chaudhari et al.	
	67	20090197612		2009-08-06	Kiiskinen, Arto	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	68	20100151866		2010-06-17	Karpov et al.	
	69	20060143066		2006-06-29	Calabria, Hermann	
	70	20120166604		2012-06-28	Fortier et al.	
	71	20040133668		2004-07-08	Nicholas III, Henry T.	
	72	20070073899		2007-03-29	Judge et al.	
	73	20060136882		2006-06-22	Noonan et al.	
	74	20070234402		2007-10-04	Khosravi et al.	
	75	20020154751		2002-10-24	Thompson et al.	
	76	20030084321		2003-05-01	Tarquini et al.	
	77	20070174490		2007-07-26	Choi et al.	
	78	20090048913		2009-02-19	Shenfield et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	79	20090181662		2009-07-16	Fleischman et al.	
	80	20020191573		2002-12-19	Whitehill et al.	
	81	20060098627		2006-05-11	Karaoguz, Jeyhan et al.	
	82	20090070379		2009-03-12	Rappaport, Theodore R.	
	83	20100318652		2010-12-16	Samba, Augustine S.	
	84	20060095517		2006-05-04	O'Connor et al.	
	85	20040260766		2004-12-23	Barros et al.	
	86	20080034063		2008-02-07	Yee, Robert	
	87	20050041617		2005-02-24	Huotari et al.	
	88	20080018494		2008-01-24	Waite et al.	
	89	20120108225		2012-05-03	Luna et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	90	20060075506		2006-04-06	Sanda et al.	
	91	20030159030		2003-08-21	Evans, Junius A.	
	92	20070257767		2007-11-08	Beeson, Curt	
	93	20060277590		2006-12-07	Limont et al.	
	94	20090036111		2009-02-05	Danford et al.	
	95	20050096024		2005-05-05	Bicker et al.	
	96	20040127208		2004-07-01	Nair et al.	
	97	20030134650		2003-07-17	Sundar et al.	
	98	20060291419		2006-12-28	McConnell et al.	
	99	20060126562		2006-06-15	Liu, Huitao	
	100	20090203352		2009-08-13	Fordon et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	101	20100041365		2010-02-18	Lott et al.	
	102	20140073291		2014-03-13	Hildner et al.	
	103	20080066181		2008-03-13	Haveson et al.	
	104	20080212751		2008-09-04	Chung, Simon	
	105	20070255769		2007-11-01	Agrawal et al.	
	106	20100121744		2010-05-13	Belz et al.	
	107	20080126287		2008-05-29	Cox et al.	
	108	20030028623		2003-02-06	Hennessey et al.	
	109	20070299965		2007-12-27	Nieh et al.	
	110	20070061800		2007-03-15	Cheng et al.	
	111	20060200663		2006-09-07	Thornton, Andrew J.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	112	20050060525		2005-03-17	Schwartz et al.	
	113	20070297378		2007-12-27	Poyhonen et al.	
	114	20090006229		2009-01-01	Sweeney et al.	
	115	20090217364		2009-08-27	Salmela et al.	
	116	20050108075		2005-05-19	Douglis et al.	
	117	20070255797		2007-11-01	Dunn et al.	
	118	20090042536		2009-02-12	Bernard et al.	
	119	20090307696		2009-12-10	Vals et al.	
	120	20040176104		2004-09-09	Arcens, Suzanne	
	121	20060099970		2006-05-11	Morgan et al.	
	122	20020120370		2002-08-29	Parupudi et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	123	20040243680		2004-12-02	Mayer, Georg	
	124	20080279216		2008-11-13	Sharif-Ahmadi et al.	
	125	20040225561		2004-11-11	Hertzberg et al.	
	126	20090016310		2009-01-15	Rasal, Digambar L.	
	127	20080096559		2008-04-24	Phillips et al.	
	128	20070130283		2007-06-07	Klein et al.	
	129	20090047989		2009-02-19	Harmon et al.	
	130	20100190469		2010-07-29	Vanderveen et al.	
	131	20040267872		2004-12-30	Serdy et al.	
	132	20050091505		2005-04-28	Riley et al.	
	133	20080320497		2008-12-25	Tarkoma et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	134	20020138599		2002-09-26	Dilman et al.	
	135	20030184793		2003-10-02	Pineau, Richard A.	
	136	20040054779		2004-03-18	Takeshima et al.	
	137	20060182137		2006-08-17	Zhou et al.	
	138	20080089303		2008-04-17	Wirtanen et al.	
	139	20090132860		2009-05-21	Liu et al.	
	140	20120144025		2012-06-07	Melander et al.	
	141	20120166364		2012-06-28	Ahmad et al.	
	142	20130072177		2013-03-21	Ross et al.	
	143	20140241342		2014-08-28	Constantinof, Cristian	
	144	20070201502		2007-08-30	Abramson, Nathan	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	145	20050163320		2005-07-28	Brown et al.	
	146	20060114821		2006-06-01	Willey et al.	
	147	20080178300		2008-07-24	Brown et al.	
	148	20090049156		2009-02-19	Aronsson et al.	
	149	20080168275		2008-07-10	DeAtley et al.	
	150	20090320110		2009-12-24	Nicolson et al.	
	151	20090065571		2009-03-12	Jain, Deepak	

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	1310401A	CN		2000-02-22	Wang, Di Xing		
	2	1878160A	CN		2006-12-13	Jiang, Yong		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	3	2012047275	WO		2012-04-19	Raleigh, Gregory G. et al.		
	4	101127988A	CN		2008-02-20	ZTE Corporation		
	5	1503548 A1	EP		2005-02-02	FG Microtec GmbH		
	6	3148713 B2	JP		2001-03-26	ATR Kankyo Tekio Tsushin Kenkyusho		
	7	2009-218773	JP		2009-09-24	Advanced Telecommunication Research Institute Inte		
	8	2006093961	WO		2006-09-08	Kyocera Wireless Corp.		
	9	2007-318354	JP		2007-12-06	Fujitsu Ten Ltd.		
	10	2007126352	WO		2007-11-08	Telefonaktiebolaget LM Ericsson		
	11	2009-212707	JP		2009-09-17	Fujitsu Ltd.		
	12	2008-301121	JP		2008-12-11	Kyocera Corp.		
	13	101335666A	CN		2008-12-31	Hangzhou H3C Technologies Co., Ltd.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	14	101080055A	CN		2007-11-28	Tencent Technology (Shenzhen) Co., Ltd.			
	15	2009-232107	JP		2009-10-08	Fujitsu Ltd.			
	16	2009-111919	JP		2009-05-21	Kyocera Communications Systems			
	17	2009008817	WO		2009-01-15	Ericsson			
	18	2002045315	WO		2002-06-06	Micromuse			
	19	2009091295	WO		2009-07-23	Telefonaktiebolaget LM Ericsson			
	20	2002093877	WO		2002-11-21	Nokia Corp.			
	21	2006004784	WO		2006-01-12	Japan Communications Inc.			
	22	2005339247A	JP		2005-12-08	Secured Communications			
	23	2006155263A	JP		2006-06-15	NEC Corporation			
	24	1345154A	CN		2002-04-17	Datang Microelectronics Tech. Co.			

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	25	2006-197137	JP		2006-07-27	NTT Docomo Inc.		
	26	2006-344007	JP		2006-12-21	Hitachi Ltd.		
	27	2005083934	WO		2005-09-09	Research In Motion Limited		
	28	2007120310	WO		2007-10-25	Qualcomm Inc.		
	29	2003017063	WO		2003-02-27	Apogee Networks		
	30	2002067616	WO		2002-08-29	Sonera Oyj		
	31	2011002450	WO		2011-01-06	Alcatel-Lucent USA Inc.		
	32	2003017065	WO		2003-02-27	Apogee Networks		
	33	1545114	EP		2005-06-22	Alcatel		
	34	1887732	EP		2008-02-13	Huawei Technologies Co., Ltd.		
	35	2007065	EP		2008-12-24	Huawei Technologies Co., Ltd.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP041D1C1

	36	2006-041989	JP		2006-02-09	Fujitsu Ltd.		
	37	1289326	EP		2003-03-05	Motorola, Inc.		

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	Dixon et al., "Triple Play Digital Services: Comcast and Verizon (Digital Phone, Television, and Internet), August 2007	
	2	3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; IP Flow Mobility and seamless WLAN offload; Stage 2," Release 10, Document No. 3GPP TS 23.261, V1.0.0, March 2010	
	3	3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO)," Release 9, Document No. 3GPP TS 24.312, V9.1.0, March 2010	
	4	Ahmed et al., "Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS)," 2010 IEEE	

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	10/10/2017

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	Rudy, Andrew J.
Serial No.:	15/287,597	Art Unit:	3687
Filed:	October 6, 2016	Conf. No.:	4727
Title:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems		

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

RESPONSE

In response to the Office Action dated November 6, 2017, the no-fee deadline for response being February 6, 2018, please enter the following response in the above-identified application:

A Listing of the Claims begins on page 2.

Remarks begin on page 6.

IPR2025-01572
Apple EX1002 Page 722

LISTING OF THE CLAIMS

Without prejudice and without surrender of any subject matter, please amend the claims as follows:

1. (Canceled).

2. (Previously Presented) A method of operating a network system, the method comprising:
receiving a first request from any first device in a plurality of similar wireless end-user devices, the first request for a secure device credential,
performing a verification step of one or more device identifiers supplied by the first device, and,
upon a successful verification in the verification step,
generating a secure device credential for the first device,
associating the secure device credential with one or more device identifiers of the first device, and
securely sending the secure device credential to the wireless end-user device;
based at least in part on the secure device credential, negotiating a secure message link between a message link server in the network system and a device link agent in the first device;
receiving, over the secure message link, a second request from the first device, the second request for a secured application credential, for any first application identified from a plurality of device applications registered to use wireless network communications, the second request comprising a general application credential for the first application; and
in response to the second request,
generating, based on the identified first application and the secure device credential, a first secured application credential unique to the first device, and
sending the first secured application credential to the first device over the secure message link.

3. (Previously Presented) The method of claim 2, further comprising, in response to receiving the first request and prior to performing the verification step, returning to the first device a network system credential that is verifiable through a trusted certificate authority.

IPR2025-01572
Apple EX1002 Page 723

4. (Previously Presented) The method of claim 2, wherein generating a secure device credential for the first device comprises encrypting the credential with a key known by at least one element of the network system.

5. (Previously Presented) The method of claim 2, further comprising routing a network message to the identified first application over the secure message link, using the first secured application credential to indicate that the identified first application is to receive the network message.

6. (Previously Presented) The method of claim 2, wherein the first secured application credential is a run-time application credential.

7. (Previously Presented) The method of claim 6, further comprising receiving, from the device link agent over the secure message link, the run-time application credential, and evaluating the run-time application credential at an element of the network system.

8. (Previously Presented) The method of claim 7, further comprising, in response to evaluating the run-time application credential, returning a network policy setting over the secure message link to the device link agent, the network policy setting applicable to the first application.

9. (Previously Presented) The method of claim 7, wherein the element of the network system is an authentication server, the network system further comprising an application credential database coupled to the authentication server and storing secured application credentials, including the first secured application credential.

10. (Previously Presented) The method of claim 2, further comprising based on a first device event, refreshing the first secured application credential to create a different secured application credential unique to the first device, and sending the different secured application credential to the first device, the different credential superseding the first

IPR2025-01572
Apple EX1002 Page 724

secured application credential.

11. (Previously Presented) The method of claim 2, further comprising, in response to the second request, verifying that the general application credential matches a known-application credential for the first application.

12. (Previously Presented) The method of claim 11, wherein the known-application credential is uploaded to the network system via an application developer service design center.

13. (Previously Presented) The method of claim 11, further comprising obtaining the known-application credential from an app store.

14. (Previously Presented) The method of claim 2, the verification step further comprising evaluating a subscriber identifier associated with one or more wireless end-user devices, including the first device.

15. (Previously Presented) The method of claim 14, further comprising generating the secure device credential based at least in part on one or more of the device identifiers and also on the subscriber identifier.

16. (Previously Presented) The method of claim 2, further comprising forwarding network messages to the first application on the first device over the secure message link, based on the first secured application credential.

17. (Previously Presented) The method of claim 2, wherein the secure device credential is a credential associated with a service processor on the first device, the method further comprising confirming the identity of the service processor based at least in part on the secure device credential.

18. (Previously Presented) The method of claim 2, wherein a first subscriber is associated with both the first device and with a second wireless end-user device, the method further

IPR2025-01572
Apple EX1002 Page 725

comprising the network system generating, based on the identified first application and a second secure device credential associated with the second device, a second secured application credential unique to the second device.

19. (Previously Presented) The method of claim 2, wherein generating the first secured application credential comprises creating a combination of the general application credential and the secure device credential.

20. (Previously Presented) The method of claim 19, wherein the combination comprises a hash.

IPR2025-01572
Apple EX1002 Page 726

REMARKS

Claims 2-20 are pending and stand rejected by the Office Action dated November 6, 2017. Claim 1 was previously canceled. In view of the remarks below, Applicant respectfully requests reconsideration.

Claim Rejections – 35 U.S.C. § 112

In section 6, the Office Action rejected claims 2-20 under 35 U.S.C. § 112(a), as failing to comply with the written description requirement. Applicant respectfully traverses the rejection, based at least on the following non-exhaustive specification passages cited below that describe the elements of the claimed invention.

The Office Action states that the phrase "a secure device credential" in line 7 of claim 2 appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures. The Office Actions states that the phrase "one or more device identifiers of the first device" in lines 8-9 of claim 2 appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures. Support for these claim elements can be found, e.g., in the specification excerpts below, taken from paragraphs [00230] and [00233] of the specification and associated figures:

> [00230] In some embodiments, **before service processor 115 of end-user device 100 participates in device-assisted services, it enrolls with service controller 122**. In the enrollment process, **service controller 122 (using, e.g., credentialing application server 146, a network element such as authentication credential server 220, etc.) allocates a device credential to service processor 115**. In some embodiments, the credential is one or more of a certificate, a key, a shared secret, a password, a hash, a shared algorithm, or any other item of information that allows service controller 122 to confirm the identity of service processor 115. **After service controller has allocated the device credential, service controller 122 can use the device credential when it needs to authenticate service processor 115**, such as, for example, before end-user device 100 sends device-based usage reports to gateway application server 138.
>
> [00233] **FIG. 22 illustrates the steps service controller 122 (e.g., using credentialing application server 146) performs to provide a device credential to end-user device 100 in some embodiments**. At step 1030, service

IPR2025-01572
Apple EX1002 Page 727

> controller 122 receives a request for a service controller credential from end-user device 100. In some embodiments, the request comprises a device identifier and a subscriber identifier. At step 1032, service controller 122 sends the service controller credential to end-user device 100. At step 1034, **service controller 122 receives a credential signing request comprising a challenge password from end-user device 100**. In some embodiments, **the request comprises a device identifier and a subscriber identifier**. At step 1036, **service controller 122 verifies that the subscriber identifier is listed in database cluster 116**. At optional step 1038, **service controller 122 verifies the device identifier from a device table**. In some embodiments, the device table resides in database cluster 116 and contains a list of valid devices that are allowed to connect to service controller 122. At step 1040, **service controller 122 validates the challenge password using the device identifier**. At step 1042, **service controller 122 stores the device identifier in database cluster 116 as associated with the subscriber identifier associated with end-user device 100**. At step 1044, **service controller 122 generates a device credential for end-user device 100 by obtaining a primary key from database cluster 116**. At step 1046, service controller 122 **stores the device credential in database cluster 116 as associated with the subscriber identifier and the device identifier associated with end-user device 100**. At step 1048, **service controller 122 sends the device credential to end-user device 100**. In some embodiments, service controller 122 (e.g., using credentialing application server 146) comprises a simple certificate enrollment protocol (SCEP) server, and the credential is a certificate. In some embodiments, messages sent and received by service controller 122 are encrypted. In some embodiments, **the service controller credential and device credential are 2048-bit RSA public key credentials**. In some embodiments, service controller 122 and end-user device 100 communicate using a session key. [emphasis added]

The Office Actions states that the phrase "a second request" in lines 14 of claim 2 appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures. The Office Actions states that the phrase "a secured application credential, for any first application identified from a plurality of device applications registered to use wireless network communications" in lines 15-16 of claim 2 appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures. The Office Actions states that the phrase "a general application credential for the first application" in line 17 of claim 2 appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures. The Office Actions states that the phrase "a first secured application credential

IPR2025-01572
Apple EX1002 Page 728

unique to the first device" in line 20 of claim 2 appears to lack support from the descriptive portion of the specification in juxtaposition with the drawing figures. Support for these claim elements can be found, e.g., in the specification excerpts below, taken from paragraphs [00272], [00274], and [00275] of the specification and associated figures:

> [00272] FIG. 35 illustrates an example embodiment of another procedure that a service controller may use to validate that an application installed on an end-user device is authentic. At step **1200**, the **service controller receives a signed application credential comprising an installed-application credential and a device credential from the end-user device**. The device credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. In some embodiments, **the signed application credential comprises a combination of the installed-application credential and the device credential (e.g., a hash). At step 1202, the service controller uses the device credential to process the signed application credential to obtain a first application credential**....
>
> [00274] FIG. 37 illustrates an example embodiment of another procedure that a service controller may use to validate that an application installed on an end-user device is authentic. At step **1220**, **the service controller obtains an application credential from a trusted source, wherein the application credential is associated with the installed application**. The application credential may be any type of credential, such as, for example, a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. In some embodiments, the trusted source is a marketplace, an app store, an application author, a distributor, or a reseller. At step **1222**, **the service controller generates a signed application credential using the application credential and a device credential stored in local memory**. In some embodiments, local memory is database cluster **116**. In some embodiments, the device credential is a certificate, a key, a shared secret, a password, a hash, or a shared algorithm. At step **1224**, **the service controller sends the signed application credential to the end-user device**. In some embodiments, after sending the signed application credential to the end-user device, the service controller receives a message from the end-user device providing information about the authenticity of the application installed on the end-user device.
>
> [00275] FIG. 38 illustrates an example embodiment of end-user device **100** for implementing **access network policy specific to a device application program**. In the embodiment of FIG. 38, end-user device **100** includes communication

IPR2025-01572
Apple EX1002 Page 729

> modem **880**, memory that includes **application program store 830 and application credential and policy store 810**, application execution environment **850**, and application policy control **820**. Communication modem **880** enables end-user device **100** to communicate over at least a first access network. Application program store **830** stores a run-time application program. Application credential and policy store **810** stores a known-application credential associated with a known application program and a known application access network policy associated with the known-application credential. In some embodiments, the run-time application credential is stored with the run-time application program. In some embodiments, the known-application credential is a security certificate, signature, or hash for the known application program. In some embodiments, **end-user device 100 is further configured to obtain the known-application credential from a network element by way of a secure data connection between end-user device 100 and the network element**. [emphasis added]

Applicant respectfully submits that the invention as claimed is fully supported by the original written description of the Application. Applicant requests that the rejection for lack of written descriptive support be withdrawn.

Claim Rejections – 35 U.S.C. § 103

In section 9, the Office Action rejected claims 2-20 under 35 U.S.C. § 103(a) as being unpatentable over US 8,146,142 to Lortz (hereinafter, "Lortz"). Applicant respectfully submits that a *prima facie* case of obviousness is lacking in the rejection.

Lortz addresses a problem inherent in "introducing" two devices by proposing an out-of-band registration process, followed by an in-band cryptographic registration process to issue credentials to an enrollee. Lortz, col. 6, ll. 1-59. After introduction, "registered applications" can use the introduction service to obtain application-specific configuration data and cryptographic keys for their own sessions. *Id.*, col. 11, l. 15 to col. 12, l. 10.

To Applicant's understanding, Lortz focuses on an identification of an "enrollee" and thus does not "associate the secure device credential with one or more device identifiers of the first device," as claimed. Further, the use by applications of the introduction service to obtain configuration data based on an application identifier is not "a request for a secured application

IPR2025-01572
Apple EX1002 Page 730

credential" as claimed—the application merely seeks and receives configuration data and keys for its own secure sessions. Accordingly, there is also no step in Lortz of "generating, based on the identified first application and the secure device credential, a first secured application credential unique to the first device."

Finally, the Office Action states that "Official Notice is taken that different application credentials as recited by Applicant used in a secure communication network has been common knowledge in the network system art." Applicant is unclear as to what "different application credentials as recited by Applicant" means in this statement, and therefore traverses the Official Notice as Applicant does not know what feature is alleged to have been in the prior art. A specific prior art reference would be helpful to Applicant in evaluating the state of the art at the time of filing.

Applicant also notes that the rejection does not specifically address the dependent claims. To Applicant's reading, these claims contain further inventive concepts not described by Lortz—for instance a device credential encrypted with a key know to the network system (claim 4), routing a network message to an application using the first secured application credential (claim 5), the secured application credential being a run-time application credential (claim 6), receiving the run-time application credential and evaluating it in the network (claim 7) and performing further steps in response to such evaluation (claims 8 and 9), refreshing based on a device event the secured application credential (claim 10), etc. Applicant respectfully requests that the rejection for obviousness be withdrawn.

IPR2025-01572
Apple EX1002 Page 731

CONCLUSION

Applicant respectfully requests entry of this response. The application is believed to be in condition for allowance, and a Notice of Allowance is hereby respectfully requested. If the Examiner has any questions or needs any additional information, the Examiner is invited to contact the undersigned.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: May 6, 2018

By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: May 6, 2018 By: /Ann Taylor/
Ann Taylor

IPR2025-01572
Apple EX1002 Page 732

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP041D1C1

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	5915226	A	1999-06-22	Martineau	
	2	6246870	B1	2001-06-12	Dent et al.	
	3	6535949	B1	2003-03-18	Parker, Kenneth W.	
	4	6591098	B1	2003-07-08	Shieh et al.	
	5	6603975	B1	2003-08-05	Inouchi et al.	
	6	6760417	B1	2004-07-06	Wallenius, Jukka	
	7	6959202	B2	2005-10-25	Heinonen et al.	
	8	7031733	B2	2006-04-18	Alminana et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	9	7120133	B1	2006-10-10	Joo et al.	
	10	7165040	B2	2007-01-16	Ehrman et al.	
	11	7315892	B2	2008-01-01	Freimuth et al.	
	12	7548875	B2	2009-06-16	Mikkelsen et al.	
	13	7584298	B2	2009-09-01	Klinker et al.	
	14	7607041	B2	2009-10-20	Kraemer et al.	
	15	7610057	B2	2009-10-27	Bahl et al.	
	16	7620383	B2	2009-11-17	Taglienti et al.	
	17	7627600	B2	2009-12-01	Citron et al.	
	18	7656271	B2	2010-02-02	Ehrman et al.	
	19	7668966	B2	2010-02-23	Klinker et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	20	7681226	B2	2010-03-16	Kraemer et al.	
	21	7688792	B2	2010-03-30	Babbar et al.	
	22	7693107	B2	2010-04-06	De Froment, Eric	
	23	7721296	B2	2010-05-18	Ricagni, Giuseppe	
	24	7774412	B1	2010-08-10	Schnepel, Soenke	
	25	7797019	B2	2010-09-14	Friedmann	
	26	7805522	B2	2010-09-28	Schlüter et al.	
	27	7809372	B2	2010-10-05	Rajaniemi, Jaakko	
	28	7813746	B2	2010-10-12	Rajkotia, Purva R.	
	29	7835275	B1	2010-11-16	Swan et al.	
	30	7853656	B2	2010-12-14	Yach et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	31	7873346	B2	2011-01-18	Petersson et al.	
	32	7873540	B2	2011-01-18	Arumugam, Avin	
	33	7882560	B2	2011-02-01	Kraemer et al.	
	34	7930553	B2	2011-04-19	Satarasinghe et al.	
	35	7979889	B2	2011-07-12	Gladstone et al.	
	36	8024424	B2	2011-09-20	Freimuth et al.	
	37	8060017	B2	2011-11-15	Schlicht et al.	
	38	8090361	B2	2012-01-03	Hagan, Guy R.	
	39	8149748	B2	2012-04-03	Bata et al.	
	40	8234583	B2	2012-07-31	Sloo et al.	
	41	8306741	B2	2012-11-06	Tu, Ihung	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	42	8340625	B1	2012-12-25	Johnson et al.	
	43	8346923	B2	2013-01-01	Rowles et al.	
	44	8355570	B2	2013-01-15	Karsanbhai et al.	
	45	8392982	B2	2013-03-05	Harris et al.	
	46	8401968	B1	2013-03-19	Schattauer et al.	
	47	8407472	B2	2013-03-26	Hao et al.	
	48	8413245	B2	2013-04-02	Kraemer et al.	
	49	8495743	B2	2013-07-23	Kraemer et al.	
	50	8504574	B2	2013-08-06	Dvorak et al.	
	51	8531995	B2	2013-09-10	Khan et al.	
	52	8549173	B1	2013-10-01	Wu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	53	8559369	B2	2013-10-15	Barkan	
	54	8588240	B2	2013-11-19	Ramankutty et al.	
	55	8594665	B2	2013-11-26	Anschutz, Thomas	
	56	8620257	B2	2013-12-31	Qiu et al.	
	57	8676682	B2	2014-03-18	Kalliola, Janne	
	58	8818394	B2	2014-08-26	Bienas et al.	
	59	8843849	B2	2014-09-23	Neil et al.	
	60	8849297	B2	2014-09-30	Balasubramanian	
	61	8868727	B2	2014-10-21	Yumerefendi et al.	
	62	8891483	B2	2014-11-18	Connelly et al.	
	63	8929374	B2	2015-01-06	Tönsing et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	64	9064275	B1	2015-06-23	Lu et al.	
	65	9137286	B1	2015-09-15	Yuan	
	66	9286469	B2	2016-03-15	Kraemer et al.	
	67	9286604	B2	2016-03-15	Aabye et al.	
	68	9459767	B2	2016-10-04	Cockcroft et al.	
	69	9609459	B2	2017-03-28	Raleigh, Gregory G.	

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	20020099848	A1	2002-07-25	Lee, Hoon	
	2	20040024756	A1	2004-02-05	Rickard, John Terrell	
	3	20060101507	A1	2006-05-11	Camenisch, Ja L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	4	20070171856	A1	2007-07-26	Bruce et al.	
	5	20100284388	A1	2010-11-11	Fantini et al.	
	6	20110004917	A1	2011-01-06	Saisa et al.	
	7	20110252430	A1	2011-10-13	Chapman et al.	

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	1098490	EP	A2	2001-05-09	Nortel Networks Ltd.		
	2	1942698	EP	A1	2008-07-09	Apple Inc.		
	3	2026514	EP	A1	2009-02-18	Nokia Siemens Networks		
	4	2007129180	WO	A2	2007-11-15	Nokia Corp.		
	5	2010128391	WO	A2	2010-11-11	Bridgewater Systems Corp.		

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

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	Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009	
If you wish to add additional non-patent literature document citation information please click the Add button Add			

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	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

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	/James E. Harris/	Date (YYYY-MM-DD)	2018-05-06
Name/Print	James E. Harris	Registration Number	40013

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 record s.

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.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 098 490 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.05.2001 Bulletin 2001/19

(51) Int Cl.7: **H04L 29/06**

(21) Application number: **00309735.9**

(22) Date of filing: **03.11.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **05.11.1999 US 434628**

(71) Applicant: **Nortel Networks Limited**
Montreal, Quebec H2Y 3Y4 (CA)

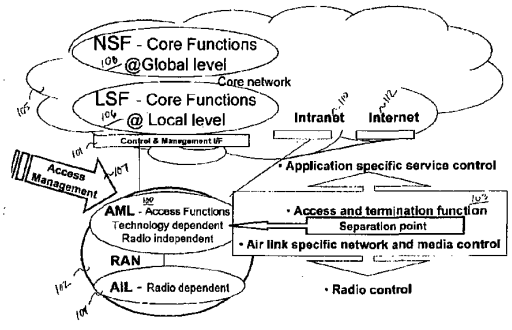
(72) Inventors:
- **Amin, Rajesh B.**
  Desoto, Texas 75115 (US)
- **Hanley, Donald V.**
  McKinney, Texas 75075 (US)
- **Morrow, Glenn C.**
  Plano, Texas 75075 (US)
- **Allahyar, John**
  Dallas, Texas 75252 (US)

(74) Representative: **Mackenzie, Andrew Bryan et al**
Sommerville & Rushton,
45 Grosvenor Road
St Albans, Herts. AL1 3AW (GB)

(54) An architecture for an IP centric distributed network

(57) A method and system to for a communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising: a network service function layer within the wireless network. The network service function layer can include: a policy management server; an authorization server; a service accounting server; an authentication, authorization and accounting server; an unified directory within a directory server; a security gateway; and a mobility manager. The architecture also includes a local service function layer associated with the network service function layer. The local service function layer can include: an access accounting server; an authentication, authorization and accounting server; a security gateway; a policy enforcement server; a mobility manager; a network management server; and a wireless gateway. The architecture also includes an access management layer associated with the local service function layer. The access management layer can include: a location tracking server; a connection management server; a protocol server; an access management server; a policy enforcement server; a network management server; and a resource management server. The architecture also includes an access interface layer associated with the access management layer. The access interface layer can include: a channel management server; a policy enforcement server; an administration and maintenance server; and a radio frequency server.

Figure 1



Printed by Jouve, 75001 PARIS (FR)

EP 1 098 490 A2

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 744

Description

FIELD OF THE INVENTION

[0001] The invention relates generally to computers and, more particularly, to an architecture for an Internet Protocol centric distributed network and a method and apparatus for such a network.

BACKGROUND OF THE INVENTION

[0002] Recently, wireless communication devices have become more and more popular as a method of communicating from one point to another. Cellular Radio is one, and probably the most popular, method of wireless communication. The original and still, most common Cellular Mobile Telephone System is a low-powered, duplex, radio/telephone which operates between 800 and 900 mHz for TDMA and 1800 and 1900 mHz for CDMA, using multiple transceiver sites linked up to a central computer for coordination. The geographic region served by a cellular system is subdivided into areas called cells. Each cell has a central base station and two sets of assigned transmission frequencies; one set is used by the base station, and the other by mobile telephones. To prevent radio interference, each cell uses frequencies different from those used by its surrounding cells, but cells sufficiently distant from each other can use the same frequencies. When a mobile telephone leaves one cell and enters another, the telephone call is transferred from one base station and set of transmission frequencies to the next using a computerized switching system. The first cellular telephone system began operation in Tokyo in 1979, and the first U.S. system began operation in 1983 in Chicago.

[0003] The earlier system have been focused on providing mostly voice services with some capability of providing data communications as well. However, recently, the need for a network designed with other services in mind other than just voice has arisen. The network should be able to provide access to different application layer protocols such as Session Initiation Protocol, H.323, and Internet Protocol to name a few.

SUMMARY OF THE INVENTION

[0004] In contrast to the prior art, the present invention provides a distributed IP centric system and method for wireless access to an internet protocol (IP) based network, wherein the system and method is independent from technology used in accessing the network. The system also uses the application layer to send messages between the access layer and the IP network. The access layer also includes distributed IP based functionality and the flexibility to be incorporated into distributed servers on a Local Area Network (LAN). The access layer also includes the capability to support establishing and maintaining the wireless link and mobility services to the mobile station through the access layers along with simultaneous IP access to public domain services. The access layer also handles connection management independent from the hardware used (such as ATM, Ethernet, etc.).

[0005] To this end, in one embodiment the method and system include a communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising: a network service function layer within the wireless network. The network service function layer can include: a policy management server; an authorization server; a service accounting server; an authentication, authorization and accounting server; an unified directory within a directory server; a security gateway; and a mobility manager. The architecture also includes a local service function layer associated with the network service function layer. The local service function layer can include: an access accounting server; an authentication, authorization and accounting server; a security gateway; a policy enforcement server; a mobility manager; a network management server; and a wireless access gateway. The architecture also includes an access management layer associated with the local service function layer. The access management layer can include: a location tracking server; a connection management server; a protocol server; an access management server; a policy enforcement server; a network management server; and a resource management server. The architecture also includes an access interface layer associated with the access management layer. The access interface layer can include: a channel management server; a policy enforcement server; an administration and maintenance server; and a radio frequency server.

[0006] Therefore, in accordance with the previous summary, objects, features and advantages of the present invention will become apparent to one skilled in the art from the subsequent description and the appended claims taken in conjunction with the accompanying drawings.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 745

BRIEF DESCRIPTION OF THE DRAWINGS

[0007]

Figure 1 is a diagram of separating wireless access from the Core Network;
Figure 2 is a diagram of the LSF/NSF (core) Layer functional service components;
Figure 3 is a diagram of the Radio Access Network Layer functional service components;
Figure 4 is a diagram of the Mobile Terminal Layer functional service components;
Figure 5 is a diagram of Protocol layers and interactions;
Figure 6 is a diagram of Service layer interfaces;
Figure 7 illustrates the connectivity of the Access Management Layer;
Figure 8 is a diagram of AML functional components;
Figure 9 is a diagram illustrating step 1 of the access session establishment procedure;
Figure 10 is a diagram illustrating step 2 of the access session establishment procedure;
Figure 11 is a diagram illustrating step 3 of the access session establishment procedure;
Figure 12 is a diagram illustrating step 4 of the access session establishment procedure;
Figure 13 is a diagram of the service session invocation procedure;
Figure 14 is a diagram of the functional component interaction sequence flow;
Figure 15 is a diagram of an overview of an access scenario at the AIL-AML;
Figure 16 is a diagram of an QoS change request;
Figure 17 is a diagram of use of default QoS to establish call/session;
Figure 18 is a diagram of a call/session invocation request;
Figure 19 is a diagram of power up registration;
Figure 20 is a diagram of the use of default parameters; and
Figure 21 is a diagram of an example implementation of the various layers of the architecture of the preferred embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0008] The present invention can be described with several examples given below. It is understood, however, that the examples below are not necessarily limitations to the present invention, but are used to describe typical embodiments of operation. Additionally, a list of abbreviations and a glossary will be listed first to facilitate a better understanding of the invention.

Abbreviations

[0009]

AAA	Authorization Authentication Accounting
AIL	Access Interface Layer
AML	Access Management Layer
ATM	Asynchronous Transfer Mode
CDMA	Code Division Multiplex Access
CN	Core Network
COA	Care Of Address
COPS	Common Open policy Service
dB	data Base
DHCP	Dynamic Host Configuration Protocol
DNS	Directory Name System
DEN	Directory Enabled Networking
DS	Directory Server
FR	Frame Relay
HDLC	High Level Data Link Control
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDP	Local Decision Point

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 746

LSF	Local Serving Function
L1	Layer 1
L2	Layer 2
L3	Layer 3
MH	Mobile Host
MM	Mobility Manager
MPLS	Multi-protocol Label Switching
MS	Mobile Station
NGWN	Next Generation Wireless Network
NSF	Network Serving Function
OSI	Open System Interconnection
PDP	Policy Decision Point
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RF	Radio Frequency
RSVP	Resource Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
QoS	Quality of Service
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service
SS	Session Server
TCP	Transmission Control Protocol
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
UWN	Unified Wireless Network
WAG	Wireless Access Gateway

Definition of terms

[0010] UWN: The Unified Wireless Networks is the IP centric core-network consisting of LSF and NSF network components. The UWN is assumed to be independent of air interface technology. The interfaces between system components of the UWN are based on the LAN/WAN technology and uses client server architecture.

[0011] 2G: The current wireless network components are referred to as the second-generation components. The 2G-network component uses industry-defined protocols and interfaces to communicate between the system and network components.

[0012] 3G: The future wireless network components evolved from the 2G components are referred to as the third generation components. In the description of the preferred embodiment it is assumed that the 3G will be backward compatible to the 2G. For an example, 3G mobile (voice mode) terminal is capable to act as 2G mobile (voice mode) in voice call support. In addition, 3G will be able to support new standards for making a multi-media call using newly defined standards. The gateway devices may be used to support 2G and 3G components.

[0013] NG: The future wireless network components that evolve from the 3G components are referred to as the Next Generation components. The NG components are assumed to take full advantage of the IP centric network infrastructure and eliminate the need of gateway devices. End devices will become smarter with the capability of communicating without the need for the gateway or mapping functions.

[0014] NSF: The NSF is one of the network components of the UWN architecture. It consists of several system components. These components may include legacy components through the necessary interfaces or their functional equivalent suitable to the IP centric environment. Some of these components are HLR, SCP, Unified Directory, AAA server, SN, IP Service Platform (provides value added applications to the client), etc. Network Serving Function (NSF) is the global home component of the UWN that owns the mobile user's subscription.

[0015] LSF: The LSF is one of the network components of the UWN architecture. It consists of several system components. Some of these components are CS, MM, CD, DHCP, DNS, Gateway devices, etc. The Local Serving function (LSF) is the serving component of the UWN that provides services to local and visiting wireless subscriber in that area.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 747

[0016] RAN: The Radio Access Network is the system component of the wireless network that provides radio control functions used in transmitting and receiving control and data information between mobiles and core network. The RAN itself is air technology dependent. However, it is evolving to provide independent functionality towards the IP centric core network. On this basis, RAN is assumed to have distinct radio interface and access management components. The radio management components provides the radio independent functionality towards the IP centric core network.

[0017] AML: The Access Management Layer is the service layer of the RAN that consists of radio management and access management components.

[0018] AIL: The Access Interface Layer is the service layer of the RAN that consists of air link interface handling components.

[0019] WAG: The Wireless Access Gateway is the entity that interfaces with the wireless access network such as 3G RAN and provides controlling capabilities to facilitate the RAN resources to meet users' requirements such as bandwidth management and also to interface with the intranet or Internet components.

[0020] WGW: The Wireless GateWay is the entity that interfaces and provides gateway functionality between the traditional wireless access such as BSC and the IP centric network. The WGW is assumed to provide merely tunneling capabilities to transport messages such as DTAP or BSMAP between IP centric network and the traditional 2G-access controller. This definition is not used in the description of the preferred embodiment. However, it is provided just to differentiate the meaning of WGW with the WAG described earlier.

[0021] UAC: User Agent Client is the first entity within the wireless network that assumes responsibility on behalf of the user to communicate with the core network or external network components. The UAC facilitates the activities in the ingress direction. Typically, the UAC is capable of communicating to the external servers directly. However, in some instances the UAC may convey such need to the UAC proxy.

[0022] UAS: User Agent Server is the entity that receives requests from the UAC or the UAC proxy. It facilitates the activity in the egress direction.

[0023] UAC proxy: User Agent Client Proxy takes responsibilities on behalf of the UACs to send appropriate requests to the server.

[0024] UAS proxy: User Agent Server proxy is the first entity within the wireless network that assumes the terminating responsibility on behalf of the receiving user. However, it has the ability to forward or redirect the call/session to other external components. The UAS-proxy facilitates the activities in the egress direction. Typically, the UAS proxy is capable of communicating to the terminating user directly. However, in most instances the UAS-proxy just conveys such information to the UAS that in turn communicates to the end user.

[0025] Ingress: This term is used for those activities that occur in direction from the mobile host to the network.

[0026] Egress:This term is used for those activities that occur in direction from the network to the mobile host.

[0027] Outgoing call/session: This term is used as defined by the bellcore documents. This term is used for the call/session activities that originated from the mobile host and progresses to other network through the serving network.

[0028] Incoming call/session:This term is used as defined by the Bellcore documents. This term is used for the call/session activity that originates from the external network and progresses to the mobile host through the serving network.

Introduction

[0029] The distributed IP centric Wireless Internet - NGWN architecture is centered around IP mobility management, call/session management, and network management. The scope of the description of the preferred embodiment is to explore call/session management services.

[0030] The call/session management services consist of three functions. These functions are: 1) establishing an access session between the mobile host and the serving network; 2) an invocation of a service session by the end user; and 3) facilitating network resources to establish point to point or point to multi-point virtual connection.

[0031] The establishment of an access session attaches the mobile host to the serving network. During the establishment, subscribers' are authenticated and granted either a specifically requested, or a default, bandwidth with the desired quality of service. Once the access session is established, the mobile host becomes IP capable and can reach, or be reached, any other devices. The access session remains active while the mobile host is attached to the serving network..

[0032] Once the access session is established, the user can invoke a service session. The user is provided with user capabilities and network preferences to use services from the serving network or externally accessed services. Although the user is provided with many choices of service invocation, the one of the main components is call/session control services. The management of call/session control is distributed to a set of appropriate servers (functions) within the access management and Local Service Function (LSF) network service layers. This distribution allows access relevant activities to be coupled with the access dependent service layers, and policy decision making activities coupled with the access independent layers. The services originated at the application level are configured with the appropriate application servers at the LSF service layer. In addition, call/session control services are part of the access management

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 748

services that aids to facilitate in establishing point to point and point to multi-point virtual connections.

[0033] The main components of the Unified Wireless Networks (UWN) consist of IP mobility management components, call/session management components, network management control, and gateway devices that interface with other systems supporting different protocols. The network management control functionality is also important but dependent on the full definition on the other components. The gateway functionality is also required along with the other appropriate components of the UWN.

[0034] The description of the preferred embodiment focuses on the functional components of the call/session management services. These functional components are distributed in distinct network service layers based on their role. The network access and user service related functional components are distributed in the access management and service management layers respectively. Further; the service management layer is distributed into a local network service layer and a global network service layer.

[0035] Thus, realization of functional components and their appropriate separation into access and service layers have allowed separating network access and service management functions from the media transport. This enabled the end user to have choice of using serving network services or to use external Internet services. Detailed procedures to establish the access session and invoke the service session are discussed below.

Objectives/Requirements

[0036] The call/session management tasks are expected to achieve objectives for three basic functions. These functions are comprised of first, establishing, maintaining and terminating an *access session* between mobile host and the serving network. Second, providing network services to the mobile host that allows a mobile host to establish a *service session*. And third, facilitating transport resources of the serving network to establish a *transport session* based on the mobile hosts' need of bandwidth with a desired quality of service. The desired objectives to achieve these three functions are described below. Moreover, the call/session management functions are real time sensitive where access of decision making information and propagation delay through the network infrastructure plays an important and critical role. Additional objectives related to performance, capacity, and scalability are also identified for real time and other similar issues.

Access, Service, and Transport Session Objectives

[0037] These three basic functions of the call/session management services are identified and elaborated to distinctly depict the differences within the Wireless Internet.

Access Related Objectives

[0038] An establishment of an access session enables the mobile host to establish a point of presence at the local serving network. During access session establishment, subscriber management services are executed. These services include admission policy control decision, provisioning of default air link resources, and establishing the virtual packet channel that allows mobile hosts to interface with the external Internet network. The following paragraphs describe the access related objectives in detail.

[0039] Any access dependent requirements for subscriber management services should be identified. The subscriber management services include authentication, authorization, usage selection and usage constraints associated with subscriber.

[0040] User authentication and authorization are based on digital certificates/signatures, and is provided by an authentication server.

[0041] Usage selection and user constraints are based on the subscriber profile and network policy.

[0042] Provisioning the local serving functions with access and usage profile in order to provide allowed access and usage services to the mobile host.

[0043] Handling of flexible bandwidth provisioning and supporting requirements.

[0044] Handling of accounting requirements based on flat rate, per packet, time used, and/or Quality of Service provided.

[0045] Handling of data speed requirements of up to 144 kb/s for vehicular users, up to 384 kb/s for outdoor to indoor mobility, and up to 2 Mb/s for indoor and Pico cell environments. Handling of Quality of Service requirements.

Service Session Related Objectives

[0046] The service session enables an end user to use services provided by the serving network. Also, an end user can use the serving network services to dynamically change network transport resources. That will allow an end user

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 749

to access globally available network services at the required bandwidth for a desired quality of service. The following paragraphs describe a few objectives:

[0047] Identify serving network services to facilitate use of access network application servers to provide services independent from the subscriber's home network.

[0048] Identify any interaction needed in providing global network services that are based on service level agreements between other networks (home or third party).

[0049] Identify serving networks' role in enabling end user to form a private network within the scope of serving the Wireless Internet.

[0050] Identify scheme for reporting network resource usage.

[0051] Establishing and managing voice, paging, Short Message Service (SMS), and circuit and packet data oriented services (e.g. multi-media conference, on-line subscription, etc.).

[0052] Service capabilities related to information and functionality such as dynamic negotiation of QoS, use of Intranet service and use of communication resources.

Transport Related Objectives

[0053] The transport session activities enable the mobile host to use the network's air and virtual packet channel path resources. The following paragraphs describe a few identified objectives.

[0054] Establishing bearer connection path for an air link and virtual packet channel using serving network's resources.

[0055] Facilitating Point to Point, Point to Multi-point and Multi-point to multi-point connection.

[0056] Facilitating use of underlying network infrastructure resources such as ATM, FR, or Ethernet.

[0057] Facilitating use of payload coding/decoding task identified by the payload mediation function of the local serving function.

Other Related Objectives

[0058] The following paragraphs describe a few more important objectives.

[0059] Performance objectives :

[0060] Minimum packet delay; ITU recommends roundtrip delay less than 300 ms.

[0061] Minimum packet loss, such that no noticeable degrade in voice quality and the performance of fax.

[0062] Maximum throughput via a virtual connection

[0063] Optimized bandwidth distribution

Challenges

[0064] An identification of the Call/Session management functions and objectives for the newly defined NGWN are relatively straightforward. However, the feasibility of such objectives to implement and achieve quality of traditional networks in the newly defined Wireless Internet is not an easy task;. it is a paradigm shift. It involves many unknowns and challenges. An attempt is made here to list such challenges in this section along with the solutions in subsequent sections.

[0065] Identify interfaces and signaling objectives between mobile host and network components. More precisely between:

[0066] Mobile host and network's access management layer (AML) functional components to establish access session.

[0067] Mobile host and network's local service layer functional (LSF) components to establish service session.

[0068] Mobile host and home network service layer functional components (NSF) to establish Virtual Home Environment.

[0069] Achieve distributed transparencies for applications.

[0070] Achieve optimized information caching significant to established clusters and domains.

[0071] Reduce dependencies for availability and reliability of network components due to network problems, server problems and faulty software.

[0072] Achieve scheme to reach neighboring domains directly avoiding hierarchical intervention.

[0073] Identify both connection oriented and transaction-oriented services.

[0074] Identify inter-working between non-IP access network and IP-based core network.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 750

Architectural Framework: Emphasizing Call/Session Management components

[0075] This section establishes context for the call/session management services. An architectural framework is illustrated mainly emphasizing the functional service layers and components. It starts with separation of functional boundaries and later decomposes functional components in detail. The interfaces and interactions between network entities and inter-working between functional service layer components is described below. However, in order to illustrate the separation of functional layers and the respective inter-working between layers, the description will not flow from figure 1 through figure 8 sequentially, but will refer to the figures out of order. However, the elements are numbered consistently throughout figures 1 through 8 so as to help the understanding of the description.

Architectural overview

[0076] The NGWN/Wireless Internet is an IP centric distributed Local Area Network (LAN) based architecture. The network components in this architecture are functionally separated as required to fulfill the need of wireless telecommunication and is also suitable to integrate with other data and telecommunication networks.

[0077] The NGWN architecture provides the separation of applications/services control that interacts with the end user and management of the physical infrastructure. Figure 1 identifies the separation of wireless access 102 from the core network 105 at the access management layer 107. Figures 2 through 4 illustrate the distributed architecture with suggested functional service components. The main focus of interest is on the functional service components at the LSF 106/NSF 108 network layer and the Radio Access Network Layer 102. Figure 2 identifies the core functional service components associated with the LSF 106/NSF 108 network layer. Figure 3 identifies the access interface and access management specific functional service components. As shown in figure 2, the WAG functional components 200, 202 provide the bridge function between the local service layer 106 and the access management service layer 100.

[0078] Now referring to figures 1 and 2, the WAG component 101 that is attached to the LSF network 106 represents the access gateway point for the technology dependent functional components. Multiple access gateway points 202 can be attached to the LSF network 106. This provides flexibility in network scalability. The detailed functionality of the WAG components is represented by the Access Management Layer components 100 and shown in figure 3. The LSF 106/NSF 108 service layer functional components on one side of the WAG provide the application specific controlling functions. The access side 104 of the WAG provides the technology dependent access functions.

[0079] The access points 200 and 202 shown in figure 2 as the Wireless Access Gateway, separate the network in two distinct layers. First, the LSF106 /NSF 108 network layer that consists of common core functional service components required for telecommunication network. Second, the Radio Access Network layer that is partitioned into Access Interface Layer (AIL) 104 and Access Management Layer (AML) 100 consists of access interface and access management specific functional service components. Through out the description of the preferred embodiment, an access point that is attached to the LSF 106/NSF 108 (core) network layer is referred for wireless access point. The separate access point is required because of the different air technologies used for wireless access. Likewise, any other technology such as a wireline telecommunication system or a LAN based system can be attached to the LSF/NSF network layer. For different types of access points attached to the core network, the appropriate corresponding controlling core functional service components can be added and configured into the network.

[0080] The LSF/NSF service layers provide the core network functions. Some of the core network functions are listed in Appendix B. Depending on the scalability requirement of the network, the functional service components within the LSF 106 and NSF 108 network layers can be distributed or consolidated based on the desired hierarchy.

[0081] The access management layer 100 as shown in figure 3 provides the controlling functionality relevant to access management and RF management activities. Please note that the RF management activities and access management activities are part of the Radio Access Network layer 102. However, only RF management activities are closely coupled with the AIL 104 and access management 100 activities are closely coupled with the core network. Thus, it is possible to separate the access management activities from the RAN layer. Another major activity is the connection management function. The RAN also provides other associated functions such as local decision making domain specific database, resource control for radio resources, transmission facilities associated with the connection management function, and network management activities. These functions are illustrated in more detail in figure 8. The RF management function of the AML interfaces with the AIL service components and service components within the AML. It performs functions such as channel management, resource management at the AIL level, and policy decision functionality with respect to the AIL needs. The access management functions of the AML interfaces with the core components towards the network side and service components within the AML. The major access management function includes the ingress and egress activities that take place through the access point. Figure 8 shows distributed access management functions. The 'Access' function 800 provides ingress activities, while 'Termination' 802 and 'Paging' 804 functions provide an egress activities. The layer 3 protocol signaling messages between the mobile host and the serving network received at the AIL are distributed to the pre-configured functional service components. The layer 3 protocol

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 751

signaling accomplishes basic inter-working activities with the terminal device. Some of such activities include mobility management activities, location updating, radio resource selection, power control adjustments 806, and channel assignment and reassignments. Also, it may include network layer (L3) originated call control and supplementary services as traditionally used in legacy mobile systems. The AML components are pre-configured to communicate with the AIL components and tunnels appropriate signaling and data information.

The AIL components provide the radio access functions.

[0082] Now referring back to figure 1, the AML 100 is the dividing point 103 between the core network 105 and access dependent controlling functions 102 and 104. The components within the access management layer 100 take the role equivalent to the policy enforcement while the LSF 106/NSF 108 (core) service layer components provide the role equivalent to the policy decision. In order to expedite the policy decision and also to take advantage of the distributed infrastructure, the WAG (the access point attached to the LSF network) domain database is considered at the AML, which facilitates the policy and subscriber related default parameters and access related status information.

[0083] The functionality of various functional components in each service layer is out of the scope to describe in the description of the preferred embodiment. However, Appendix A provides a brief description for some of these components. The access management functional component as shown in figure 3 plays an important role in providing call/session management services. The distribution of access management component functionality along with other AML components is described in figure 8. The access management component performs ingress and egress activities. Logically, access management functions can be further distributed into access (origination) function for ingress activities and termination 802 and paging 804 functions for egress activities. These functions can be physically located in a single (access management) server 800. However, they can be distributed in different servers as they provide distinctly independent functionality. These functional service components are capable of sending/receiving application level messages (from/to user) as well as layer 3 protocol messages over IP (from/to AIL) that take place between the mobile host and the serving network. The detailed functions of these components are described later. However, a brief description is provided here to establish context.

[0084] The access management 800 of the AML takes the role of user agent in the network domain. Within the access management function 800, the access function takes the role of user agent client. With respect to the call/session management service perspective, this functional component handles ingress activities such as registration and origination. Similarly, the termination function 802 takes the role of user agent server and provides the proxy functions for egress activities. The paging function 804 is the further distribution of the egress activities that is associated with the users at the cell level 808. The location-tracking function (defined as handoff function later) handles handoff activities. The location-tracking function interfaces with the LSF service layer component - mobility manager for periodic location update, and inter system (WAG to WAG domain) and inter network domain controlling functions such as handoff.

Interfaces between network entities

[0085] The functional service components are distributed in appropriate network service layers as shown in figure 2 and figure 3 that interact with each other using various interfaces. Although the logical interface model is not shown in the figures, the lower layer (L1-L2) interfaces (shown in figure 5) are assumed to be Ethernet. The interface at the transport layer is either TCP or UDP that is based on the delay sensitivity and reliability requirement. The "other" in figure 5 indicates the support of application level framing (ALF) and support of timer associated with transport layer protocols in order to enhance transaction level capabilities such as controlling congestion and canceling transactions. Application layer protocols are text based and based on the currently being defined Internet protocols.

[0086] The logical interface model includes primary control and data path interfacing to the Wireless Internet. Unlike the LAN based application interfaces in most interfaces mentioned in this model, the air link interface is a specific interface. The mobile host interfaces at the serving network on the technology dependent air interface uses network layer protocol messaging. The radio access interface layer, as shown in figure 3, terminates the network layer air technology dependent messages. Based on the type of messages received at the access interface layer, they are distributed to the pre-configured functional components at the access management layer. Detailed procedures are explained later in the description of the preferred embodiment.

[0087] Although the details of the Mobile Terminal Layer are not discussed much in the description of the preferred embodiment, figure 4 shows an example of how the functionality of the mobile host can be separated into two layers: a wireless interface layer and a mobile application layer.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 752

Application inter-working

[0088] Figure 5 depicts the protocol layers and interactions between network entities. It establishes the main context for application interactions between various network components. It shows the protocol interfaces between OSI layers that inter-work to accommodate air interface and LAN based connectivity. The description of the preferred embodiment only focuses on activities that take place above the transport layer in case of LAN based architecture and at the network layer in case of air interface.

[0089] The following sections describe the interactions between mobile host and access network components, mobile host and local serving function components, and mobile host and home network components.

Interactions between mobile host and access network

[0090] The Access Management Layer and the Access Interface Layer are the part of the Radio Access Network. The AML service components provide the access dependent control functions. The technology dependent network layer (L3) protocol terminates at this point. The AML service components are logically distributed into different functions as shown in figure 8. A signaling distributor between AIL and AML distributes messages to the pre-configured functional components (servers). With respect to the call/session management services, the access, termination and paging functions play an important role. These components interface with the LSF service components in order to provide services to the AIL and the mobile host. The LSF service components interface with the NSF service components in order to provide services to the access management components.

[0091] The following interactions occur between the mobile host and the access management service layer:

[0092] The AML components interact with the network layer of the mobile host to establish an access session. (L3/IP between AIL and AML)

[0093] The AML components interact with the AIL components to bring the mobile host on the traffic channel.

[0094] The AML components interact through the connection management component to establish point to point protocol path that allows the mobile host to access any other IP capable devices.

[0095] The network preferred call/session control services are handled through the access management components.

[0096] Handoff, power control, and paging functions related handshakes with the mobile host are controlled by the AML components.

[0097] Interactions between mobile host and CN/LSF network service components

[0098] The LSF network service components provide specific services to the access management components during establishment of an access session and service session with the mobile host.

[0099] The subscriber management and policy decision services are provided during an access session establishment with the mobile host.

[0100] The policy decision services are provided during user session invocation.

[0101] Intranet services are provided by the LSF service components through the specialized application servers.

[0102] Interactions between mobile host and CN-NSF/Global network Service components

[0103] The NSF network service components provide services to the LSF network service components during establishment of an access session with the mobile host.

[0104] The subscriber management services are provided during an access session establishment with the mobile host.

[0105] Facilitate to publicly available server accesses.

[0106] Direct home network accesses.

[0107] Interactions between network service layers

Inter-working between service layer components

[0108] The access management layer components and the LSF/NSF service layer components are the main network components that play the significant role in controlling call/session management. The functional components within an access management layer are the edge components through which mobile users in a area accesses the core network for access establishment service, service session invocation service and intranet services or external network access services. The AML is comprised of many distributed functions. These functions are explored in subsequent sections including access (Origination: User Agent Client), termination (Termination: User Agent server), protocol servers (optionally at AML but not at LSF service layer), power control, resource control, handoff, paging, and connection management (Transport Network). The functions within LSF/NSF network service layer include service broker, session server, payload mediation, and AAA+ (accounting, authorization, and authentication) servers. The components are described in greater detail later.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 753

[0109] How these components interact with each other as well as with end user and establish an access session, service session and transport session is also described later in the text. The access function facilitate to establish an *access session* that interact with the mobility manager to provide the functionality and the context needed to grant and support the user in accessing NGWN - Wireless Intranet services. Typical access functions performed by the network domain include an establishment of an authentication, authorization, usage selection, and usage constraints. At the end of establishing access session, the serving network is configured and provisioned with the subscriber's profile to provide appropriate access role, and usage role to the end user. Further, appropriate access functions are instantiated within the access management layer that interacts with mobile host to facilitate service session invocation and monitoring usage functions of the network resources. These instantiated functions interact with the session and accounting servers during the service session. The access functions within the AML take the role of User Agent in the network domain.

[0110] The session server component of the LSF/NSF network service layer facilitates establishment and maintenance of a *service session*. It provides the functionality needed to satisfy end users' request for desired services. The functional components within the LSF/NSF network service layer provide services to the access management layer and to the end user in establishing functionality and context involved in the negotiations of parties, configuration and QoS to be associated to the execution of a service. These services are unlike the call model services that facilitate in establishing connection-less or connection oriented call/session.

[0111] The AML of a particular domain must establish an association with the session server of the LSF/NSF network service layer in order to provide call/session services to a mobile. It is possible for the AML to have association with multiple session servers. However, the AML must associate with a single session server to complete initiated transaction. It is also possible to have many transactions during call/session establishment. During each transaction the AML may use a different session server. This implies that the AML maintains call/session states.

[0112] The session server provides services such as address translation, location service, and bandwidth management and admission policy control. It interacts with the AML for instantiated access functions to provide desired call control and other session services to the mobile host.

[0113] The session server is capable of accessing any of the AML components. This enables the session server to update the domain specific local database within the AML, monitor resources and achieve flexibility (optional) to manage connections for traffic. Updating local domain database provides necessary intelligence to the AML components to perform default capabilities quickly and efficiently. Also, the session server uses services from home (global) network components (NSF) for the purpose of authentication, authorization, accounting, policy related decisions, and globally provided services. The session server performs the function of redirect server in terms of SIP context (SIP Session Initiation Protocol - RFC 2543) or similar to gatekeeper function in terms of H.323 context for the call/session control services.

[0114] The connection management component of the AML provides the function of establishing *transport session* that establishes an end-to-end virtual connection, and handles multi-point and multi-media connections. It interacts with the session and accounting servers for policy and usage monitoring and reporting functions.

Call/Session management specific: components, services, and procedures

[0115] This section describes call/session management relevant functional service components within each network service layer and services and procedures that establish access session and transport sessions. The service components within an access management layer of the RAN layer and service components within the local service layer of the LSF/NSF network services layer plays an important role in providing call/session management services.

Access Management Layer (AML) components

[0116] The AML functional component position is between the radio access interface layer and the core network components as shown in figure 1 and figure 7. The AML component performs controlling and policy enforcement functions. It controls activities that take place at the access interface layer. Also, it controls interface activities associated with the user during access session establishment and service session invocation. It controls connection management activities that establish and monitor the point to point and point to multi-point virtual packet channels.

[0117] The network and user specific preferences are executed here based on the policy decision provided by the LSF/NSF network layer service components. The local domain database is updated with limited relevant information during access session establishment and service session invocation that expedites real time critical policy decision execution. For an example, an origination request arriving at the access management server examines the requested bandwidth with the allowed default permission through the local domain database. If the requested bandwidth matches with the allowed default, an access management server facilitates the requested bandwidth through the resource control function of the AML. If the requested bandwidth is other than default, an access management server may consult

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 754

with the session server to take further action.

[0118] These functions can be physically distributed in different servers within the AML as network capacity demands. The AML functions (i.e. components) are pre-configured with the local service layer components to provide services to the mobile host during access session establishment. Additional components are instantiated and configured at the end of access session establishment. This is done based on the capabilities granted to the users and network capabilities to provide additional services.

[0119] Figure 6 illustrates how some of the components within each layer interfaces to some of the other components and is only meant to illustrate an example of the components described in detail throughout the description of the preferred embodiment.

[0120] Figure 7 illustrates the respective position of AML in Wireless Internet. Figure 8 illustrates the functional components within the AML. The functional components within the AML are pre-configured with a signaling router that interfaces between AIL and AML. The signaling packet to/from the radio access interface layer arbitrates at the signaling distribution function of the AML and distributes to the pre-configured AML components based on the type of signaling (e.g. related to call/session processing, mobility management, supplementary services, radio resource, etc.). An access function plays an important role in ingress direction while termination and the paging functions play an important role in egress direction. The access function takes the role of user agent on behalf of the end user. An access function involves in initial dialog with the mobile host. At network layer, the mobile host communicates with the access function using network layer messages. Intelligence at the access function uses local domain database in performing default services. For higher-level policy decisions, it accesses the session server at the LSF network service layer.

Activities of the AML components are described below:

[0121] **Access function** - Access function takes care of ingress related call/session management activities. These activities include registration and origination. An access function is the first signaling termination point with respect to ingress call establishment. It executes the policy enforcement functions. The access function of the AML takes the role of a user agent in a serving network. It interfaces with the mobile host to provide access session establishment service. During initial registration, it interacts with the mobility manager of the LSF network layer component that facilitates the subscriber management services. Upon successful completion of the subscriber management services through the mobility manager, the local domain database is updated with user and network preferences. The local domain database provides the local decision point functions. This expedites the domain specific activities during service session invocation and through out the active access session.

[0122] Further, an access function facilitates the establishment of a traffic path (establish PPP link) between the mobile host and the connection management component. The purpose of this action is to establish an access session between the mobile host and the serving network. The access function of the AML does this in two steps. First, the access function interacts with the RF management (resource control as shown in figure 8) component to bring the mobile on a traffic channel. Second, the access function interacts with the connection management component through which the PPP protocol messages handshake to establish IP address service point at the mobile host. The mobile host can negotiate the choice of IP address to be used; either network provided or mobile provided. This establishes the transparencies between the mobile host and the serving network. The access function informs the session server of the LSF network layer about the completion of the access session.

[0123] At this point, the session server has direct addressing capability to the mobile host to provide user capabilities and network preferences. Based on the usage and preferences granted to the mobile host, an appropriate service session manager function is instantiated within the access management layer domain. The user application interacts with the service session manager for service invocation and network service requests.

[0124] The access function takes the role of either user agent client or user agent client proxy depending on the need that is based on the capability of the mobile host. Please note that access function implies that the activities may be provided by an instantiated session server manager or handed over to the appropriate protocol servers. When the mobile host is capable to control call/session-handling activities, the mobile host takes the role of user agent client. The access function provides the role of user client proxy if requested. The mobile host has choice not to use access function as client proxy and may contact any desired client proxy or directly to the end user agent server. The mobile host keeps track of state machine. If the mobile host requests to the access function to aid in further call/session-handling activities, the access function takes the role of user agent client proxy. In this case, the access function is taking role of client proxy may interacts with the session server that provides the role of redirect server. Also, the access function can play role in two possible modes. First, an idle mode in which it provides call/session-handling transaction services when requested but do not keep track of call/session state machines. Second, an active mode, in which access function provides call/session-handling transaction services and keep track of call/session state machine.

[0125] When the mobile host is not capable of handling call/session activities, the access function receives request from the mobile host. The access function takes the role of user agent client, interacts with the session server for

EPNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 755

admission control and policy decision if required. The access function performs the outgoing call/session activities. The access function keeps track of state machine.

[0126] Termination and paging function - Termination function handles egress activities related to the incoming service session (call control activities) requests. Why do we need the termination function? In an IP environment, with the fact that each IP capable mobile host is addressed by a specific IP address, an external caller when trying to reach a mobile host in a Wireless Internet, it can reach directly without any intervention from the wireless access. However, this is only true when the mobile host is attached to the serving system using its permanent IP address. Because of the transient characteristics of the mobile host it is more suitable to assign a domain specific IP address within the Wireless Internet. In this case, once the domain specific address is made globally available by linking with the mobile host's home then the external caller only needs to find domain specific termination-proxy server. The termination-proxy server associates the current location of the callee within that domain with the current paging server (user agent server).

[0127] Thus, the termination function acts as a user agent proxy server for the user agent servers associated within the AML (notice cloud shown in figure 8). The termination function provides the first signaling termination point with respect to egress call establishment. It executes the policy enforcement functions. The local domain database provides the local decision point functions. This expedites the domain specific activities during termination service session establishment. The termination function interacts with domain database to get information for handling incoming request. If the end-user is not recognized, it interacts with the session server of the LSF component to take further action. In terms of SIP context (SIP RFC 2543), the session server performs function similar to the redirect server. Similarly, in H.323 context, the session server performs function similar to the gatekeeper. The termination function uses services from the session server and mobility server of the core network for various services that may include authentication during termination, current location information and policy-related decision.

[0128] If the end-user is recognized (i.e. registered within this domain) and the requested service is allowed, the termination function directs the request to the appropriate paging function (user agent server) to page the end-user or activate the traffic path from either standby or dormant mode. The paging functions (user agent servers) are associated with the unique cells within the access management domain serving area. The paging functional component keeps track of the call/session state machine as it is acting as a user agent server on behalf of the mobile host.

[0129] The termination and paging function interacts with the RF management server (resource manager) to establish a radio link connection. As mobile host is attached to the serving network, a domain specific IP address is already assigned. So in terms of SIP context (SIP RFC 2543), this IP address is returned in the contact header when returning response to the INVITE message. The termination or paging function interacts with the connection management function to establish a transport session.

[0130] Protocol servers (or functions) - The access management functions are closely coupled with the protocol servers or functions. The protocol functions are the different code points within the system specific to the type of protocol (such as SIP, H.225, H.245, RSVP, MPLS, etc.) used for the specific activities (such as session establishment, quality of service request, secure virtual path establishment, mobility specific, etc.). These functions can be part of the access management functions and instantiated for each service session invoked. Or, these functions can be separated in different servers and access management functions can hand over the specific requests to these servers as needed. The role of these servers varies depending on the type of protocols. For an example, in SIP context, such server provides functional role as proxy server. Similarly, in H.323 context, such server provides functional role as H.323 gateway.

[0131] The location of these protocol functions or servers is not appropriate at the LSF network layer as they are closely coupled with the access management activities. For the simplest network hierarchy, these functions or servers can be associated with one WAG (access point) domain. As network scalability increases, i.e., additional access points are added, other access points can access these servers established at a single geographically convenient location. Alternatively, it is possible to locate these protocol servers along with other Intranet application servers.

[0132] Once access management hand over request to the appropriate protocol servers, these servers create direct links with the end user and takes the responsibility to interact with the connection management functions to establish appropriate transport session.

[0133] Connection management function - The connection management function is the part of the AML component. It provides the third and final phase of the call/session management services that facilitates in establishing transport session. It receives transport session establishment request from the access (user agent client) function or instantiated session service manager during the outgoing service session establishment. Similarly, the termination (UAS proxy server) and/or paging function (user agent server) requests transport session establishment during incoming service session establishment. Based on the request, the connection management function facilitates to establish the point to point or point to multi-point virtual packet channel. The connection management function monitors and records usage activities. Like session service manager, the connection session manager is instantiated for each transport session establishment. The connection session manager for the transport session takes care of providing required quality of service and use of appropriate network infrastructure as described earlier.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 756

[0134] **Configuration Manager** - the configuration management function at the AML service layer facilitates reconfiguration of AML service layer components. It also facilitates location tracking (handoff) with addresses of neighboring location tracking components that are used for handoff activities during movement from one AML to another AML.

[0135] **LSF/NSF network service layer components** - There are many functional components that are involved in providing call/session management services. However, only some of these are significant for the purpose of the description of the preferred embodiment and described here.

[0136] **Session server** - The session server is one of the call/session management service components at the local service layer. The primary function of the session server is to interact with the AML service components to provide call/session management services. More precisely, it interacts with the access function and the termination function within the access management server of the AML service layer. Also, it interacts with the connection management function at the AML for usage monitoring and recording purpose. Once the access session is established between the mobile host and the serving access network, the access function interacts with the session server. At this time, the session server may configure the mobile host with available network preferences and users granted capabilities. Also, the session server provides important IP addresses to the mobile host (possibly using html) that can provide value-added services. The call control services are some of the many other services the mobile host can invoke. The session server at the LSF service layer along with access and termination functions at the AML service layer provides most of the call/session control services. The typical functions facilitated by the session server includes address resolution, call/session admission control, policy control decisions and access accounting control.

[0137] Other issues such as address translation and finding terminating proxy servers are not explored here. However, it is important to mention that the session server is assumed to perform functions similar to the redirect server identified within the SIP component definition (SIP RFC 2543). An identification of functionality for admission policy control and bandwidth management is the challenge with respect to the 3rd generation infrastructure. In addition to these, the role of session server in providing location-based applications and its interactions with the mobility manager server is also a challenge. These issues are differed at this time.

[0138] **Database management (directory services)** - The call/session functions related to a subscriber are typically based on the subscriber's profile. Such information in wireless network is typically centrally located at the subscriber's home NSF layer or at global level. In order to take advantage of the distributed network, subscriber's profile and related information need to be distributed in appropriate domains. Such distribution should be to a level where access point dependent components (e.g. session server, MM server) and radio dependent components (e.g. functional components within the AML) can take necessary decision independently. Such distribution will expedite the call/session processing and reduce the lengthy delay involved in accessing centrally located database and hence improve performance.

[0139] **Call/Session management services** - The ultimate objective of the Wireless Internet is to provide the end user an access through the network, provide choice of user desired services (Intranet or external Internet, etc.), and finally, the control and monitor capability for network resources used. The call/session management services facilitate these objectives. Three basic functions were briefly identified earlier. These functions are listed in the following paragraphs again.

Establishing an access session between the mobile host and the serving network

[0140] The establishment of an access session facilitates the mobile host to attach to the serving network. During the establishment, subscribers' are authenticated and granted for requested or default bandwidth with desired quality of service. The local decision point within the access management layer is updated and appropriate service components get configured. Once the access session is established, the mobile host becomes IP capable enabling access to/from any other device. The access session remains active at all times as long as the mobile host remains attached to the serving network.

An invocation of a service session by the end user

[0141] The user can invoke a service session. The call/session control service is one of many services that the user can invoke. The session server at the LSF service layer facilitates the call/session management control activities. At this point network becomes capable of providing basic call/session control services. However, the network is also capable of providing simple to complex services.

[0142] The user is provided with user capabilities and network preferences to use desired services from the serving network or access external services. Based on the user capabilities and network preferences with respect to the type of user, the network configures itself to respond to the user service invocation.

[0143] For example, in the management of basic call/session control services, the session server manager is instantiated at the access management layer that provides the user interface for call/session control services. While at the LSF service layer, instance of a session can be created at the accounting server to handle accounting activities for

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 757

any service session. Similarly, for any other service, the appropriate session manager can be instantiated to respond to that specific desired service. The application servers are configured at the LSF service layer.

[0144] This allows the ability to keep access relevant activities coupled with the access dependent service layers, and policy decision making activities at the access independent layers. Also, this allows flexibility to provide mixture of independent services and add new services.

Facilitating network resources to establish point to point or point to multi-point virtual connection

[0145] Distinction between the call/session control services and other applications/services is emphasized throughout the specification for clarification purposes. The call/session control services are the part of the access management services that facilitate establishing point to point and point to multi-point virtual connections.

[0146] **Access session establishment** - The mobile host establishes point of attachment with the serving network. The mobile hosts on power up or during idle state periodically sends registration or location update request to the serving network. The access interface layer components facilitate an air link communication with the mobile host. Upon receiving registration request, AIL distributes it to an access management server component within the AML. The access management server consists of many functions. They are identified in figure 8. They are access, termination and paging functions. These functions have independent functional role and can be separated in different servers if network capacity demands. In this section when access management server is referenced implies an access function of the access management server. The AIL distributes signaling information to the appropriate servers depending on the type of signaling. Optionally, such distribution can be implemented at the AML.

[0147] Now referring to figure 9, the access management layer processes the registration request 900. The domain database 902 within the AML provides the local decision point to the AML components to make primary decisions. The access management server 904 checks with the domain database 902. If the mobile host 906 is already registered, mobile host's current location is updated. If the mobile host 906 is not active within this domain, the access management server sends REGISTER request to the LSF service layer component - mobility manager 908. A SIP message, REGISTER is shown for examples that access management server sends to the mobility manager 908. It includes MIN or "user at domain" location information that identifies cell information.

[0148] Although the activities performed by the mobility manager 908 will not be described in great detail, a brief outcome of this activity is described here. This is the first step in establishing an access session between the mobile host and the serving network. The mobility manager 908 receives the REGISTER message. This indicates that the subscriber needs to be authenticated for access and authorized for the requested services. The mobility manager performs this task with the help of other LSF service layer components such as AAA+, directory services, DHCP, and policy server. If the mobile host is active within the regional serving domain, the LSF service layer components provide the service functions. I.e., an authentication is done through the local AAA server, an IP address assignment through the DHCP that is suitable to the AML domain, and subscriber's default profile is updated at the AML domain database as well as at the regional domain.

[0149] Once the authentication and authorization process is complete, it is assumed that the RAN is authorized to provide access to the mobile host. Now referring to figure 10, first, the access management server 904 interacts with the RF management server 1000. The access management server 904 instructs the RF management server 1000 to assign a traffic channel. The RF management server 1000 interacts with the access interface layer components and facilitates the sending of appropriate air link messages to the mobile host. The RF management server 1000 notifies the access management server 904 once the mobile host 906 establishes the traffic channel. At this time, data link connectivity is achieved between the mobile host and AIL. Second step is to establish PPP connection between the layer 2 of the mobile host and the connection management server 1002.

[0150] The access management server 904 then starts to interact with the connection management server 1002. First, it establishes the co-relation between traffic channel and assigned IP address at the connection management server 1002. Now referring to figure 11, the access management server 1002 handshakes configure/response layer 2 PPP connection messages with the layer 2 of the mobile host through the assigned IP address at the connection management server 1002. At the mobile host 906, layer 2 establishes an IP address service point link with the layer 3 (IP layer). During this handshake, the mobile host 906 accepts the network assigned IP address or provides a desired permanent IP address instead. In case of the latter, the access management server 904 reconfigures the connection management with a new IP address and also updates the appropriate hierarchical databases.

[0151] At this point, an access session is established between the mobile host 906 and the session server 1200 at the serving network as illustrated in figure 12. The application layer at the mobile host 906 becomes IP capable and can access any IP addressable device. The air link at the layer 2 is in the active mode. This link remains active for a pre-determined time that is based on the MAC layer specification. With no activity on air link, active status of this link changes to standby mode, and later goes to the dormant mode and then the traffic channel gets released. However, the established access session at the access management service layer remains active. This access session remains

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 758

active until association of the mobile host is removed or deleted at the access management layer. When any data activity happens, either from the mobile host or from the access network, the air link turns from dormant mode to the active mode.

Invocation of service session

[0152] Now turning to figure 13, once the mobile host 906 establishes point of attachment at the session server 1200 within the serving network, the mobile host 906 becomes capable to invoke any services. The mobile host 906 can access any IP addressable device. The serving network can help provide locally or globally available services. The serving network becomes smarter and configured to provide services to the user. The default parameters are configured at the local decision points at appropriate domain levels.

[0153] At this time the network is capable to provide basic services. However, the network is capable and flexible enough to provide more complex services. A brief discussion is provided here for reference and will be explored later.

[0154] The serving network provides user capabilities and network preferences to the user. The user capabilities were determined during access session establishment as a result of executing subscriber management services. The network preferences based on network capabilities are pushed to the mobile client 906. Such preferences may include a choice of invoking different type of call/session control services (voice, data, multi-media, etc.) or value added services (Intranet services, location-based services, etc.). More over, the serving network can provide a choice to the mobile host of using the serving network as an ISP provider, or for other possible options. Some of these options are illustrated on screens 1300 and 1302 in figure 13.

Establishment of transport session

[0155] Based on the type of service session invoked, the service session manager (please refer to discussion on service session manager) notifies the connection management function to establish a virtual packet channel path. The connection session manager is instantiated by the connection management function that establishes appropriate network resources to establish requested transport session. The connection management function isolates activities from the call/session control activities. For example, it hides the underlying network topology and supports the inter-working between network layers. Based on the quality of service requirement (which is discussed below), the connection management function facilitates establishment of a path ranging from no packet control to fully dedicated virtual packet channel path. It may use different techniques to achieve the required quality of service. These techniques may include use of MPLS, RTP/RTCP, RSVP as well as other schemes. The quality of service requirements may include the following: bandwidth reservation for a data path (possible use of RSVP); end-to-end latency guarantees through the optimized IP network (possible use of MPLS); network infrastructure selection such as IP or ATM backbone (Layer 1 & 2 selection); protocol selection such as MPLS, RTP/RTCP, RSVP (based on quality of service requirements); and acceptability of loss of data (possibly establish limits on acceptable vs. unacceptable loss based on type of transport session established, such as voice, audio, video, etc.)

Call/Session procedures

[0156] The call flow procedure described here uses several scenarios to outline involvement of access function. However, certain assumptions are identified in the following paragraphs.

[0157] The Mobile host should be IP capable. For example, once the mobile host is attached to a wireless access system, the mobile host can reach any IP addressable device, server or end-user directly and transparently through the network. Also, any external user or device can reach the mobile host transparently through the network.

[0158] The mobile host can seek network services for call/session establishment or dynamic change in resource allocation using standard application protocol such as SIP or RSVP.

[0159] The RAN is IP capable. Particularly, the service components within the RAN; AIL and AML are IP capable. The PPP link is established between the mobile host and connection management component of the AML. The router between the AIL and AML will arbitrate the signaling and traffic packets before forwarding to the pre-configured IP devices of the AML components. This arbitration can be done at the AIL or at the AML depending on the choice of implementation.

[0160] The functions of the AML components are distributed based on the required function. Such functions include access, termination, handoff (location tracking), paging, power control, RF management (resource control), configuration management, and connection management. Also, local domain database for local aspects is used. It provides subscriber dependant data and local policy decision parameters for system dependant data. Alternative to these local aspects, global aspect entities such as AAA+ server and Policy Decision Point (PDP) can be accessed from the core network respectively.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 759

[0161] The AML components require assuming responsibility for the end-user as a User Agent Client and User Agent Server in an ingress and egress direction respectively.

[0162] The AML component interfaces with the core network when necessary. The core network components provide either redirect server function or value added service function to the access function.

Call/session general overview

[0163] The AML service components and the session server are the main network components that play a significant role in call/session management. The AML components are the edge components through which a mobile host in an area accesses the core network for Intranet services or external network for third-party network services or publicly available Internet services.

[0164] Thus, the AML components provide the access function. The access function establishes the functionality and the context needed to grant and support the user in accessing NGWN - Wireless Internet services. The functionality of access management server component within the AML takes the role of user agent in the network domain. Please refer to discussion on each service component.

[0165] The session server provides the call/session service function. The session server provides services to the user agent in establishing functionality and context involved in the negotiations of parties, selection of functional protocol components, configuration and QoS to be associated to the execution of a service. These services are unlike the call model services that facilitate in establishing connection-less or connection oriented call/session. Thus, the session server receives a request from the user agent and satisfies the service need. Upon access initiation or registration, the access management server component of the AML takes the role of user agent on behalf of the mobile host and interacts with the session server in establishing the requested need or service. Upon establishment of an access, appropriate network configuration takes place to serve the mobile host for its default services and network capabilities. In the process, the session service manager is instantiated that interfaces with the mobile host that satisfy the service request such as dynamic change in QoS. Please refer to the section discussing the session server.

[0166] The architecture vision is such that service requests will be facilitated appropriately by the AML components. The service session manager and transport session manager is instantiated by the access management server during access session establishment. These components provide the interface point and satisfy the end users' need and requests.

[0167] Upon terminal registration (e.g. at power up), the mobile host gets control of the radio channel and engage with a specific serving RAN in an area. The mobile hosts send registration messages to the RAN that appears at the associated access management service components. For an example, in case of a CDMA technology, a network layer IS-95 origination message is received from the mobile host to the network access interface. The AIL sends this message to the associated AML using HDLC protocol or simply in IP packets using Ethernet. The signaling IP packets are received at the edge router between AIL and AML. This router arbitrates the type of message and distributes to the appropriate AML components such as access management server, power control server, or handoff server. It is assumed that the IP security is established between AIL and associated AML, and also between identified network layers. The signaling arbitrator is configured with the appropriate IP addresses of the AML components and core network components. Thus, access related messages will be forwarded to the access management server, handoff and mobility related messages will be forwarded to the handoff server, while power control related messages to the power control server, and so on. The data packets will be distributed to the connection management server.

Exemplary Functional Component Interaction Sequence Flow

[0168] Although the functions of related service components and their interactions are described earlier, figure 14 provides functional component interaction sequence flow. The following paragraphs describe a general overview for these sequences.

[0169] Sequence 1 is described as when the network layer (L3) of the mobile host sends the registration request (e. g. at the power up) to establish a point of presence at the serving network. The access function of the AML service layer receives this request.

[0170] Sequence 2 comes into play when the access function at the AML service layer communicates with the mobility manager at the LSF service layer. The mobility manager performs several functions for which it may communicates with other functional components at the LSF service layer and/or with NSF service layer in order to provide subscriber management services. In this process the mobility manager may communicate back to the mobile host through the AML service layer to authenticate the mobile host.

[0171] Sequence 3 gets traversed when registration is completed, the mobility manager facilitates to download information such as a subset of user specific default parameters and allowed service options to the AML domain database. Such information provides local decision point to expedite future service invocation procedures if necessary.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 760

[0172] The access function at the AML service layer communicates with the RF management server in sequence step 4. For simplicity, the RF management server is not shown in this figure. The RF management server performs procedure to assign traffic channel.

[0173] Sequence 5 designates informing the access function upon completion of traffic channel assignment.

[0174] The access function of the AML service layer communicates with the connection management server in sequence 6. It facilitates to establish relation between traffic channel and assigned IP address. Then, the access function negotiate with the mobile host at the layer 2 through the connection management server of the AML service layer to establish PPP connection and IP address selection. The mobile host may accept the network provided IP address or mobile host may provide its permanent IP address to use.

[0175] The mobile host communicates back to the access function of the AML service layer in sequence 7 indicating accepted IP address assignment. The access function facilitates the necessary changes relative to the selected IP address at the AML domain and/or at the LSF service layer database.

[0176] Upon establishing PPP link between the mobile host and the connection management server, the access function at the AML service layer communicates to the session server in sequence 8 to download necessary information to the mobile host.

[0177] The session server downloads necessary information to the mobile host in sequence 9. The information includes: end user's capabilities that derived as a result of providing subscriber management services during access session establishment, and network preferred preferences for which network is configured to provide optimum service. Also, the session server communicates with the connection management to provision default bandwidth and required quality of service requirement corresponding to the end user.

[0178] The sequence 10 indicates the service invocation by the mobile host. The sequence 10' (10 prime) indicates an service invocation (e.g. origination) form the network layer of the mobile host. In this case, with respect to SIP, the access function at the AML service layer provides the function similar to the user agent client (UAC). The sequence 10 indicates an service invocation from the application layer of the mobile host. In this case, with respect to SIP, the mobile host application layer provides the function similar to the UAC. Based on the end user invocation of specific use of service, the mobile host has multiple options: it can reach directly to the callee (destination end user, i.e., e.g. user agent server in SIP context); it can reach to the other domain network. In SIP context, it can reach to a user agent server proxy that can terminate to the appropriate user agent server; or it can reach to the serving network's provided appropriate protocol server. In SIP context, it can reach to the user agent client proxy. The user agent client proxy can facilitate the further action to provide necessary resources and forward service session establishment request to the callee.

[0179] If the user chooses to use network provided appropriate protocol servers, then the appropriate protocol server receives the service session invocation request in sequence 10A and 10'A. The protocol server communicates with the session server that arbitrates to the appropriate controlling entity. For an example, in SIP context, the user agent client proxy will communicate with the Redirect server. Likewise, in H.323 context, the H.323 gateway will communicate with the gatekeeper (GK). The other GW performs similar functionality provided by the user agent client proxy in SIP context or H.323 gateway in H.323 context. Such gateways may include PSTN gateway, and similar others.

[0180] Sequence 10B, 10' B is the response from the session server. The session server provides information that required to appropriately forward the service session request to the callee or to the destination.

[0181] Sequence 10C, 10' C indicates when the session server at the LSF service layer or the access function at the AML service layer communicates with the connection management server to allocate allowed bandwidth and provide selected quality of service for the transport session. Such allocation will be committed upon completion of the signaling negotiation between end parties.

[0182] Sequence 10D, 10'D is the forwarding request go out to the appropriate destination.

[0183] Sequence 11 designates when the forwarding request arrives at the user agent server proxy in SIP context, or at the H.323 gateway in H.323 context, then, such entities performs necessary functions to validate for admission control, identifying location of the end user and forwards request to the end user. Similarly, the other gateway will provide the same functions.

Protocol choices

[0184] The list of network preferred protocol preferences could be provided to the mobile host during access session establishment. The access management functions at the AML and the session server at the LSF network layer facilitate the end user with varieties of options based on the type of user's capability, subscribed options, and network preferred protocol preferences. Based on the choice of user invocation, appropriate protocol servers are accessed to establish service session. If the end user is not capable of selecting protocol options, the end user can access the access management functions. This is also a traditional way of handling request from the mobile host. The access management functions interact with the session server to determine the appropriate protocol function and facilitate the selected

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 761

capability components that can establish the service session. The request is hand over to the appropriate server to establish service session.

[0185] This scheme provides the support of any protocol. For an example, the SIP (SIP RFC 2543) and H.225 (H.225 - Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems) & H.245 (H.245 - Control Protocol for Multimedia Communication) protocol stack can be supported independently and transparently. Also, legacy protocols can be supported in the same fashion.

Wireless access scenarios

[0186] Two paths are illustrated in figure 15. The first facilitates control of the air 1500 and the virtual packet channel path 1502. The second facilitates signaling interactions 1504 with the core network to establish session and allocation of local resources. The two distinct channels through which traffic data flows are identified in the following paragraphs.

One through the air link and another through the virtual packet channel

[0187] The virtual packet channel 1502 can be established through all the routers along the data path using RSVP (following PATH - RESV signaling sequence between routers). Thus, the control of the virtual link and dynamic bandwidth changes can be obtained by using RSVP processed at each router along the data path. However, the control of the air link is not trivial. This is because of two reasons. First, the data transformation at the connection management 1506 does not distinguish data from signaling and thus, does not process the signaling protocol. The RSVP signaling is merely transported through the wireless access point to the end terminal. Thus, it becomes the end terminal's responsibility to interact with the access point to allocate or modify the bandwidth necessary for the air path. This leads to the second point where bandwidth adjustment requires a unique signaling handshake between the IP Mobile host 1508 and the AIL-AML interface 1510.

Control of session establishment and resource allocation

[0188] Within the wireless access point, the client agent for the end user performs several functions. Some of these functions include interactions with the core network 1512. The user agent (client 1514 or server 1516) performs the role of policy enforcement while the core network 1512 performs the role of policymaking decisions. Depending on the implementation choice, interactions related to the policy may be performed locally or at the core network 1512. It may be practical to distribute default parameters and the subscribers' allowed resource allocation at the time of registration to the local domain database. In this case the policy enforcement function that is a part of the user agent (access management server), performs decisions based on the local decision point (LDP) 1518.

[0189] IP capable end terminals 1520 can communicate with each other transparently. However, the wireless access point plays an important role in establishing the air link path. An intervention at the wireless access point can occur several times during the communication. These scenarios are identified in the following paragraphs.

Scenario 1

[0190] As shown in figure 16, the IP capable end terminals 1508, 1520 are in active state. Assume terminal A 1508 is attached to the wireless access side. Terminal B 1520 is somewhere else on the Internet. Terminal B 1520 sends an INVITE message directly to the terminal A 1508 using the currently used call ID to modify an active call/session with different quality of service parameters than what is included in the SDP. Terminal A 1508 needs to send a request 1600 to the access system to modify the established air link 1500.

Scenario 2

[0191] Figure 17 shows the case of a termination. When the distant client 1520 sends a message 1700, for example, an INVITE message, to the AML 1510, the message ends up at the user agent proxy server. The policy enforcement points and call admission control functions take place at the user agent proxy server. The user agent proxy server may need to access the subscriber related or the system level policy decision database. Such databases can be located locally or at some central location. The subscriber dependent database can be accessed through the local database 1518 (domain dB) for validity, profile check and current cell location if available or may be accessed through AAA server centrally located within the core network. Similarly, system level policy decisions such as allocation of subscriber requested bandwidth with respect to the availability can be checked by the proxy server by accessing local policy decision database or globally located database.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 762

Scenario 3

[0192] Figure 18 shows the call/session invocation request scenario. Though an IP mobile host 1508 is capable of establishing a call/session with another external device 1520 transparently without interaction of AML 1510, it is possible that in many cases the IP mobile host 1508 may request the AML 1510 to establish such a call/session. An example of such cases may include where a mobile host 1508 wants to establish a multicast call/session; it that case, it would request the AML 1510 to establish such a session. This is important mainly due to the bandwidth limitation of the air link 1500. The AML 1510 would facilitate the multicast of packets to as many sessions as needed. Another example is where trigger based services are incorporated that allow mobiles to invoke pre-established value added services offered by a local service provider or a local Intranet.

Scenario 4

[0193] Figure 19 shows the power up registration scenario. The power up is one case when the AML 1510 is accessed to establish an air link 1500 and establish access session. Once the air link 1500 is established, the mobile host 1508 can stay in active or dormant state. In any of these cases, the subscribers' profile is kept in a local database (domain dB) 1518. QoS policy and policy enforcement points are distributed in the access (user agent client) function for ingress and terminating user agent proxy for egress activities. Depending on the QoS requested, that include bandwidth requirements at the default level.

Scenario 5

[0194] Figure 20 shows the scenario where default parameters are used and no intervention is required. That means the mobile user 1508 can establish a session with an external user 1520 using default QoS parameters provisioned during access session establishment. In egress, the user agent proxy server will use default parameters to establish call/session with the user 1508 within the domain of AML 1510.

[0195] Figure 21 illustrates an example implementation of the architecture of the preferred embodiment. As shown, one access management layer 2100 can have one or more access interface layers 2102 and one local service function layer 2104 can have one or more access management layer 2100. In addition, local service function layer 2106 is also depicted with one or more access management layers 2108, which in turn have one or more access interface layers 2110. Additionally, the local service function layers 2104 and 2106 are shown to be connected to a network service function layer 2112 through either a LSF firewall 2114, the public Internet 2116 and a NSF firewall 2118, or through a private link 2120. The LSFs 2104, 2106 would use the private link 2120 if the NSF belonged to the same service provider and would use the firewalls 2114, 2118 if the NSF belonged to a different service provider.

[0196] Moreover, NSF 2122 is connected to NSF 2112 through a private link 2124, through a service level agreement link 2126 or through another NSF firewall 2128, the public Internet 2116 and the original NSF firewall 2118. Similarly to the LSF/NSF connections, the two NSFs 2112, 2122 would use the private link 2124 if the two NSFs belonged to the same service provider, the service level agreement link 2126 if the two NSFs had a service level agreement and the firewalls 2128, 2118 if the two NSFs belonged to two different service providers.

[0197] In addition, LSFs 2130, 2132, private link 2134, LSF firewall 2136, access management layers 2138, 2142, and access interface layers 2140, 2144 are depicted in the same format as the other components on the right side of figure 21 for simplicity purposes. However, the network could be arranged in countless ways and still withhold the relationships described above.

Conclusion

[0198] It is understood that several modifications, changes and substitutions are intended in the foregoing disclosure and in some instances some features of the invention will be employed without a corresponding use of other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 763

Appendix A: Service layer functional components

This section elaborates some of the functional components that are distributed in network service layers. The definitions given here are of generic. However, relevant details to the call/session management services are described in the specification.

Policy management & Policy enforce server - The policy management server defines business and service concerns, and more precisely, policies for users and network devices. It distributes policies to the network devices to enforce the policies defined by the network administrator. It provides policy decisions to control network behavior provided to the user. The policy enforcers are respectively at the lower layer to the policy management at appropriate network devices. These devices communicate with the policy management server using COPS protocol. The policy relevant information can be distributed at the appropriate hierarchy network layer in order to expedite the real time critical decisions.

Authentication server - The authentication server is the core network component. The mobility manager facilitates the authentication process for the mobile host. The authentication server is reachable through the AAA+ server that provides the common protocol for Authentication, Authorization, and Accounting activities. The authentication function is provided based on the digital certificates/signatures.

Directory server - The directory server stores the user service profile and policy in a database. The directory server communicates with other network components such as policy management server using LDAP protocol. The directory server uses Directory Enabled Networking (DEN) scheme. The DEN scheme takes an advantage of information already stored in directories.

DHCP - In an IP centric NGWN – Wireless Internet, a mobile host must be initially assigned a specific IP address that is appropriate to the network domain to which the mobile host is attached. If the mobile host moves to a new network domain, a new IP address must be assigned. The Dynamic Host Configuration Protocol provides such mechanism through which an IP address is allocated to the attached mobile host. The mobility manager component of the LSF service layer facilitates this procedure.

DNS – NAI DNS - The Domain Name System is the software that allows name to

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 764

number mapping. The name richweb is the 47.161.113.52 and vice versa. This is achieved through the DNS. The DNS is a hierarchy. There are small number of root domain name servers that are responsible for tracking the top-level domains and who is under them. The root domain servers between them know about all the people who have name servers that are authoritative for domains under the root. In the NGWN – Wireless Internet the DNS hierarchy is established based on the user's current location.

Mobility Manager - The mobility manager functional component is the part of the core network component. It facilitates to provide subscribers' management services during the access session establishment between the mobile host and the serving network. It also facilitates the inter-domain handoff activities.

Access Accounting server - The access accounting server is the core network component. The session server that facilitates to configure service session invocation, that also facilitates the instance for that service session at the accounting server to record the usage activities. The access accounting server is reachable through the AAA+ server that provides the common protocol for Authentication, Authorization, and Accounting activities.

AAA+ - The AAA+ server provides the common protocol access to the network clients to access Authentication, Authorization, and Accounting servers. Currently, the DIAMETER and RADIUS protocols are under evaluation for the AAA+ server access.

Network management - The network management functions at the different network layer hierarchy provide appropriate management functions. The management functions take care of business and service oriented concerns. Ideally these functions can be distributed to the core network for business decision (policy management) and service session related activities and at the AML for the network resources and transport session related activities. These functions include fault management, configuration management, accounting management performance management, and security management.

Call Server - The call server is the core network component. It takes the role of media gateway controller. It controls signaling gateway and media gateway components that interface with the PSTN.

Session server - Please refer to text above describing session server.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 765

Location tracking - The location tracking is the part of the access management layer component. It keeps track of the mobile host's location movement activities in the WAG domain. It facilitates the handoff activities between cells within the WAG domain. Also, it facilitates in inter-WAG domain handoff activities. The neighboring WAG domain information can be exchanged directly. It interacts with resource manager for the purpose of maintaining radio link and Care Of Address (COA) relationship. Also it interacts with the domain database server to update the end-user's location.

Power Control function - Power control function handles all power control related activities. It performs the necessary algorithm to manipulate special situations, which may occur due to interference or adjustment during the start of a call. It interacts with resource manager for the purpose of maintaining power level of the radio link.

Connection management server - The connection management server handles activities to establish virtual packet channel through the serving network. It gets instructions from the access management server. For each service session created, a transport session manager is also instantiated. The transport session keeps track of usage activities based on the instruction provided either per packet, per byte, time in active session, or flat time. It facilitates to establish point to point or point to multi-point transport session.

Access management server - Please refer to text above for access and termination-paging function.

RF management - The RF management server is the access management layer component. It facilitates the controlling function for the radio dependent activities. It interfaces with the access management layer components. Also, it interfaces with the access interface layer components.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 766

Appendix B: Core network functions

The LSF/NSF network layer consists of core functional service components required for telecommunication network. This section identifies the major core network functionality expected from the LSF/NSF network layer functional service components shown in Figure 2. Some of the core network functions are described in the following paragraphs.

Serving domain specific address assignment.

Policy decision based on subscriber's profile, assigned network preferences, and available network resources.

Network management control function.

Subscriber management services during access session establishment that at least include authentication and authorization.

Providing subscriber's capabilities and network preferences in serving end user.

Configuring appropriate application servers or facilitating functional service components based on the subscriber's default services or invoked services.

Usage data collection and accumulation of network resources and recording.

Handoff activities to support continuous mobility between multiple access points.

Claims

1. A method for a first user to communicate in an Internet Protocol (IP) centric distributed network with a plurality of service layers providing a plurality of functions associated with each of the service layers, the method comprising:

   accessing the network to establish a point of presence at an access management layer and a core portion of the network and to designate a default amount of bandwidth and a plurality of default setup parameters;
   invoking service through a session server on the network to establish an amount of network resources requested by the first user; and
   establishing a transport session to create and manage a connection from the first user to a destination address.

2. The method of claim 1 wherein the plurality of service layers includes a network service function layer.

3. The method of claim 1 wherein the plurality of service layers includes a local service function layer.

4. The method of claim 1 wherein the plurality of service layers includes an access service function layer.

5. The method of claim 3 wherein the local service function layer is independent of a specific access technology used for the first user to communicate to the network.

6. The method of claim 4 wherein the access service function layer accommodates a plurality of technologies used for the first user to communicate to the network.

7. The method of claim 1 wherein the invocating service through the session server includes providing a list of a

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 767

plurality of functions available to the first user.

8. The method of claim 7 wherein the plurality of functions available to the first user are based on capabilities of the first user and a plurality of network preferences.

9. The method of claim 8 wherein the session server also provides addressing of any appropriate server to contact for each of the plurality of functions available to the first user.

10. The method of claim 7 wherein the session server contacts an accounting server through an Authorizing, Authentication and Accounting server and initiates an appropriate record of resources committed to the first user.

11. The method of claim 10 wherein the accounting server sends information to an accounting accumulator at the network service layer.

12. The method of claim 10 wherein the session server instructs a connection management server to record usage information according to resources used by the first user.

13. The method of claim 12 wherein the usage information includes at least one of the group consisting of: time used by first user, packets used by first user, flat rate for each access by first user or bytes used by first user.

14. The method of claim 2 wherein the network service layer includes a mobility manager that provides handoff services to the first user when the first user leaves the local service function layer for another local service function layer.

15. The method of claim 3 wherein the local service layer includes a mobility manager that provides handoff services to the first user when the first user leaves an access management layer for another access management layer.

16. The method of claim 3 wherein the access management layer includes a location tracking server that provides handoff services to the first user when the first user leaves a first cell in a first access interface layer for another cell in another access interface layer.

17. The method of claim 1 wherein a session server reserves any quality of service parameters and an amount of bandwidth requested by the first user.

18. The method of claim 1 wherein an access and termination function at an access management layer reserves any quality of service parameters and an amount of bandwidth requested by the first user.

19. The method of claim 1 further including sending communications from an application layer at the first user wherein an user agent client resides at the first user.

20. The method of claim 1 further including sending communications from a layer 3 at the first user wherein an user agent client resides at an access management layer of the access layer.

21. The method of claim 1 further including an user agent server associated for each of a plurality of access interface layer of the access layer.

22. The method of claim 1 further including an user agent server that acts as a gateway by converting incoming protocols of incoming communications to a protocol understood by the first user.

23. The method of claim 1 further including an user agent server that delivers incoming protocols of incoming communications to the first user when the incoming protocol is understood by the first user.

24. The method of claim 1 wherein the session server further provides admission control functions and address resolution to an user agent client and an user agent client proxy at a SIP protocol server.

25. The method of claim 1 wherein the session server further provides admission control functions and address resolution to a H.323 terminal and a H.323 gateway at a H.225 protocol server.

26. The method of claim 1 wherein the network includes a connection management server that can transport commu-

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 768

nications on a plurality of backbone infrastructures.

27. The method of claim 1 wherein the network includes a connection management server that can transport communications on a point to point basis.

28. The method of claim 1 wherein the network includes a connection management server that can transport communications on a point to multi-point basis.

29. The method of claim 1 further including providing the requested amount of network resources by utilizing a connection management server that utilizes a plurality of protocols to deliver a requested quality of service for latency.

30. The method of claim 1 further including providing the requested amount of network resources by utilizing a connection management server that utilizes a plurality of protocols to deliver a requested bandwidth.

31. The method of claim 1 further including deciding policy parameters at a core network level.

32. The method of claim 31 further including enforcing policy parameters at an access management level.

33. The method of claim 1 wherein a plurality of access management layer components interact with a network layer of the first user to establish an access session.

34. The method of claim 1 wherein a plurality of access management layer components interact with a plurality of components to bring the mobile host on the traffic channel.

35. The method of claim 1 wherein a plurality of access management layer components interact through a connection management component to establish point to point protocol path that allows the first user to access any other IP capable device through a serving network.

36. The method of claim 1 wherein a plurality of network preferred call/session control services are handled through a plurality of access management components.

37. The method of claim 1 wherein handoff, power control, and paging functions related handshakes with the first user are controlled by a plurality of access management components.

38. The method of claim 1 wherein the first user interacts with a plurality of protocol servers and access management service layer components.

39. The method of claim 38 wherein the plurality of protocol servers and access management service layer components interact with a plurality of components at the local service function layer.

40. The method of claim 1 wherein a plurality of components at a local service function layer provide specific services to a plurality of access management components during establishment of an access session and service session with the first user.

41. The method of claim 1 wherein the accessing includes providing subscriber management and policy decision services for the first user.

42. The method of claim 1 wherein policy decision services are provided for the first user during user session invocation.

43. The method of claim 1 wherein Intranet services are provided to the first user by a local service function layer through specialized application servers.

44. The method of claim 1 wherein the first user interacts with a plurality of global network service components

45. The method of claim 1 wherein the accessing further includes a network service function layer providing services to a local service function layer.

46. The method of claim 1 further including providing subscriber management services during an access session

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 769

establishment for the first user.

47. The method of claim 1 further including facilitating publicly available services.

48. The method of claim 1 further including facilitating direct home network accesses.

49. A communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the network comprising:

a plurality of network service function layers within the wireless network;
a first set of a plurality of local service function layers associated with one of the plurality of network service function layers within the wireless network;
a first set of a plurality of access service function layers associated with one of the plurality of local service function layers; and
a second set of a plurality of access service function layers associated with a second of the plurality of local service function layers.

50. The communications network of claim 49 wherein at least two of the plurality of network service function layers belong to a first wireless network service provider and are connected through a private link.

51. The communications network of claim 49 wherein at least two of the plurality of network service function layers belong to two different wireless network service providers and are connected through a private link governed by a service level agreement.

52. The communications network of claim 49 wherein at least two of the plurality of network service function layers belong to two different wireless network service providers and are connected through a public link.

53. The communications network of claim 49 wherein the network service function layer includes a mobility manager that manages a handoff when the first user leaves one of the plurality of access service function layers and enters another of the plurality of access service function layers.

54. The communications network of claim 49 wherein at least one of the plurality of network service function layers and at least one of the local service function layers reside in a single entity.

55. The communications network of claim 49 wherein the first set of the plurality of local service layers includes a session server

56. The communications network of claim 55 wherein the session server provides a list of a plurality of functions available to the first user.

57. The communications network of claim 56 wherein the plurality of functions available to the first user are based on capabilities of the first user and a plurality of network preferences.

58. The communications network of claim 56 wherein the session server provides addressing of any appropriate server to contact for each of the plurality of functions available to the first user.

59. The communications network of claim 56 wherein the session server contacts an accounting server through an Authorizing, Authentication and Accounting server and initiates a record of resources committed to the first user.

60. The communications network of claim 59 wherein the accounting server sends information to an accounting accumulator at one of the plurality of network service layers.

61. The communications network of claim 59 wherein the session server instructs a connection management server at the first set of a plurality of the local service layer to record usage information according to resources used by the first user.

62. The communications network of claim 61 wherein the usage information includes at least one of the group consisting of: time used by first user, packets used by first user flat rate for each access by the first user or bytes used

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 770

by first user.

63. The communications network of claim 59 wherein each of the plurality of network service layers includes a mobility manager that provides handoff services to the first user when the first user leaves one of the first set of the plurality of local service function layers for another of the first set of the plurality of local service function layers.

64. The communications network of claim 59 wherein at least one of the plurality of the network service layers includes a mobility manager that provides handoff services to the first user when the first user leaves one of the first set of the plurality of access management layers for another one of the first set of the plurality of access management layers.

65. The communications network of claim 59 wherein the session server reserves any quality of service parameters and an amount of bandwidth requested by the first user.

66. The communications network of claim 59 wherein an access and a termination functions at one of the first set of the plurality of access management layers reserves any quality of service parameters and an amount of bandwidth requested by the first user.

67. The communications network of claim 49 further including an application layer that sends communications from the first user and an user agent client residing at the first user.

68. The communications network of claim 49 further including a layer 3 at the first user that sends communications to the network and an user agent client residing at one of the first set of the plurality of access service function layers.

69. The communications network of claim 49 further including an user agent server associated for each of a plurality of access interface layer at the first set of the plurality of access service function layers.

70. The communications network of claim 69 wherein the user agent server acts as a gateway by converting incoming protocols of incoming communications to a protocol understood by the first user.

71. The communications network of claim 69 wherein the user agent server delivers incoming protocols of incoming communications to the first user when the incoming protocol is understood by the first user.

72. The communications network of claim 59 wherein the session server further provides admission control functions and address resolution to an user agent client and an user agent client proxy at a SIP protocol server.

73. The communications network of claim 59 wherein the session server further provides admission control functions and address resolution to a H.323 terminal and a H.323 gateway at a H.323 protocol server.

74. The communications network of claim 59 further including a connection management server at a access management layer within one of the first set of access service function layers and wherein the connection management server can transport communications on a plurality of backbone infrastructures.

75. The communications network of claim 74 wherein the connection management server can transport communications on a point to point basis.

76. The communications network of claim 74 wherein the connection management server can transport communications on a point to multi-point basis.

77. The communications network of claim 74 wherein the connection management server provides a requested amount of network resources by utilizing a plurality of protocols to deliver a requested quality of service for latency.

78. The communications network of claim 74 wherein the connection management server provides a requested amount of network resources by utilizing a plurality of protocols to deliver a requested bandwidth.

79. The communications network of claim 49 further including a core network lever including the plurality of network service function layers and the first set of the plurality of local service function layers and wherein the core network layer decides policy parameters.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 771

80. The communications network of claim 49 further including an access management layer within the first set of access service function layers and wherein the access management layer enforces policy parameters.

81. A communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising:

a network service function layer within the wireless network, wherein the network service layer comprises a plurality of interconnected servers including:

a policy management server;
an authorization server;
a service accounting server;
an authentication, authorization and accounting server;
an unified directory within a directory server;
a security gateway; and
a mobility manager;

a local service function layer communicably linked with the network service function layer within the wireless network, wherein the local service function layer comprises a plurality of interconnected servers including:

an access accounting server;
an authentication, authorization and accounting server;
a security gateway;
a policy enforcement server;
a mobility manager;
a network management server; and
a wireless gateway;

an access management layer communicably linked with the local service function layer, wherein the access management layer comprises a plurality of interconnected servers including:

a location tracking server;
a connection management server;
a plurality of protocol servers;
a RF management server which includes power control, traffic control and channel assignment;
an access management server includes access, termination and paging;
a domain database server which provides a local decision point to expedite service invocation for the first user;
a policy enforcement server;
a network management server; and
a resource management server; and

an access interface layer communicably linked with the access management layer, wherein the access interface layer comprises a plurality of interconnected servers including:

a channel management server;
a policy enforcement server;
an administration and maintenance server; and
a radio frequency server.

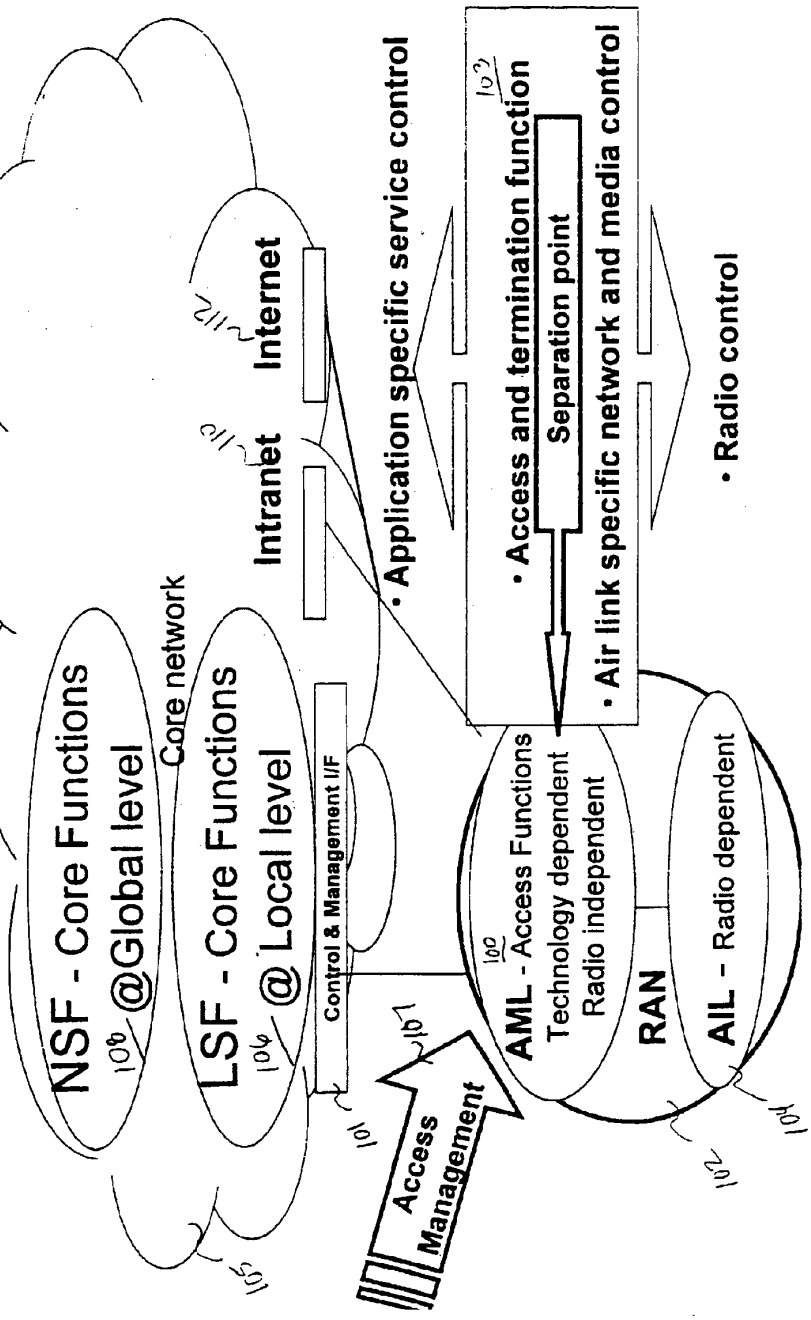
82. The communications network architecture of claim 81 wherein the access management layer provides policy enforcement.

83. The communications network architecture of claim 81 wherein the local service layer provides policy decision functions.

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 772

FIGURE 1



BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 773

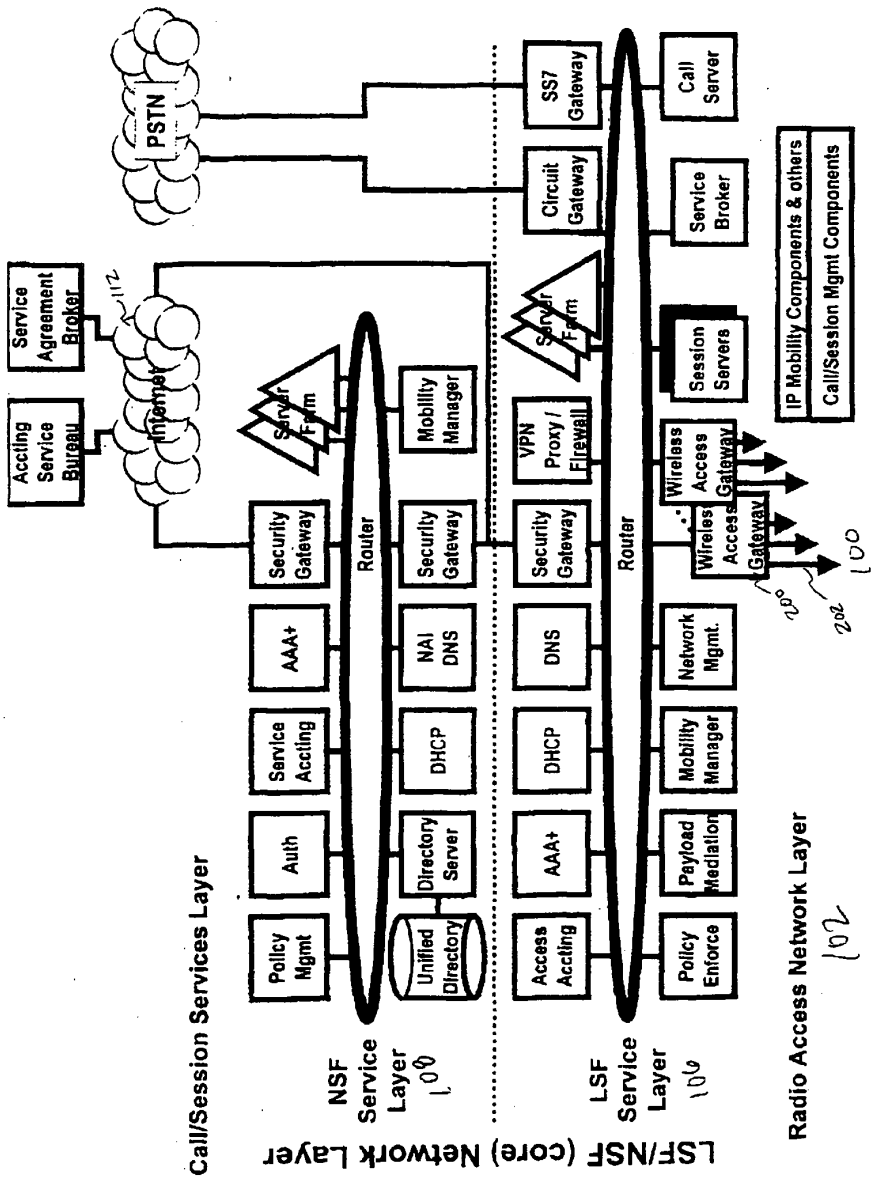


FIGURE 2

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 774

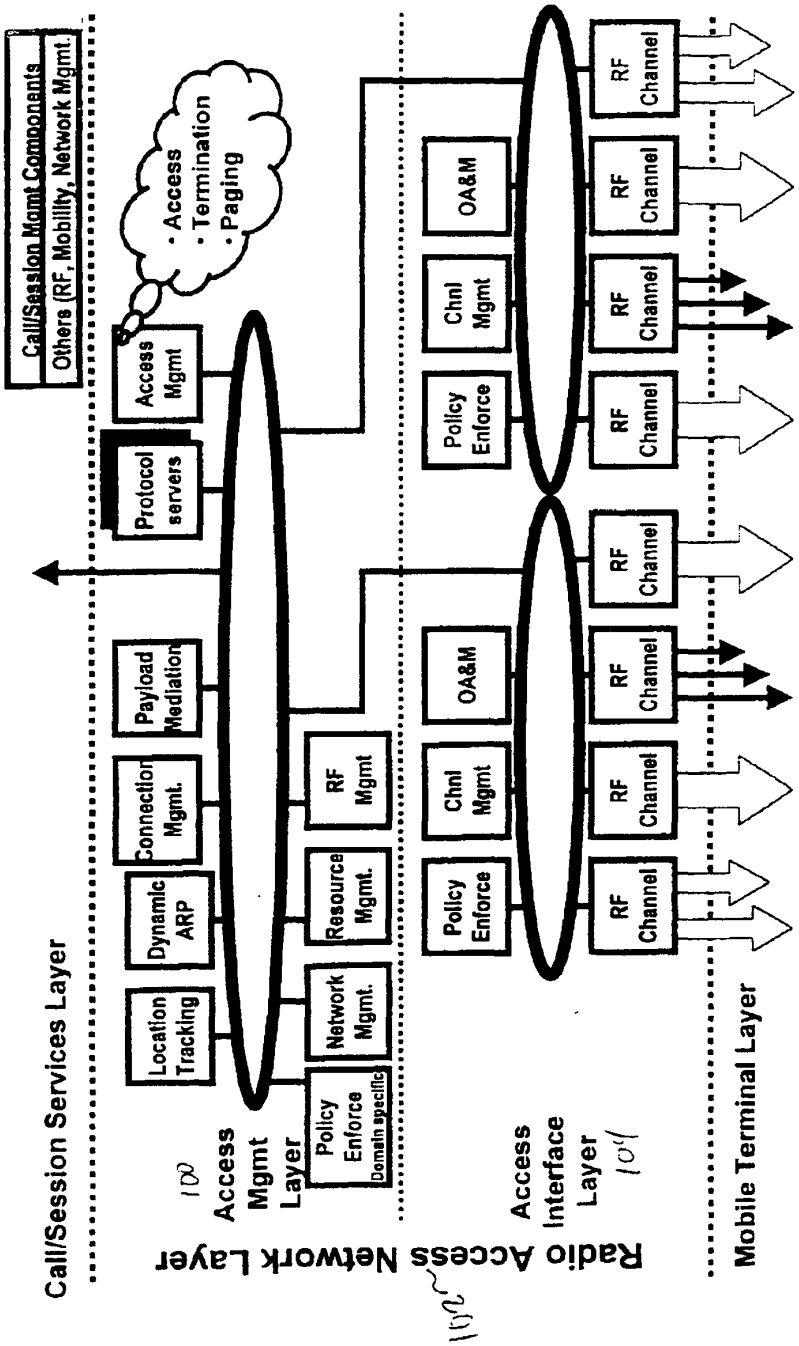


FIGURE 3

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 775

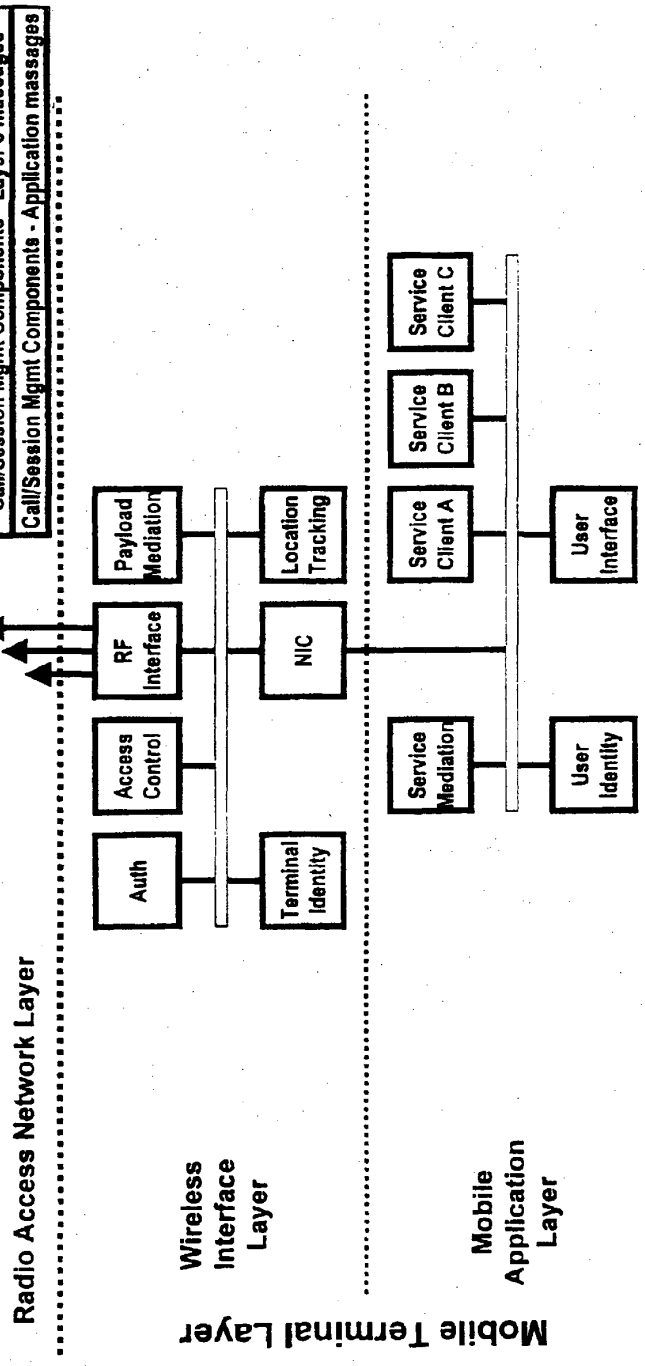


FIGURE 4

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 776

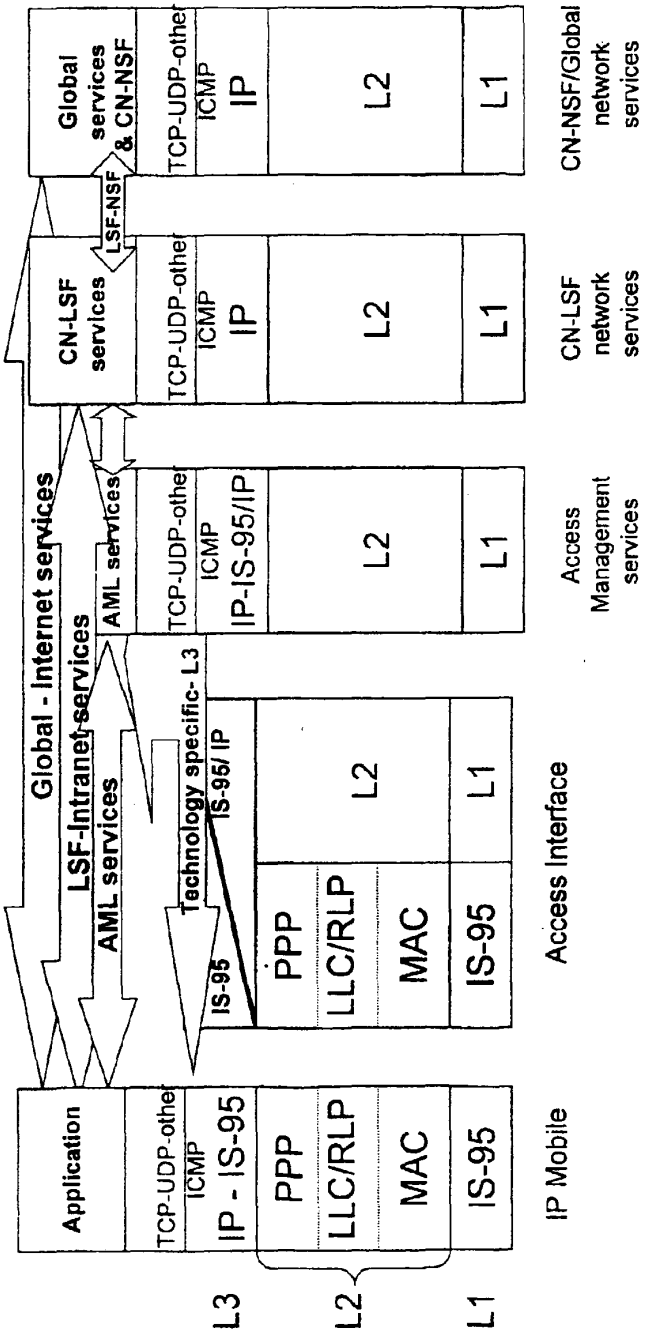


Fig. 5

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 777

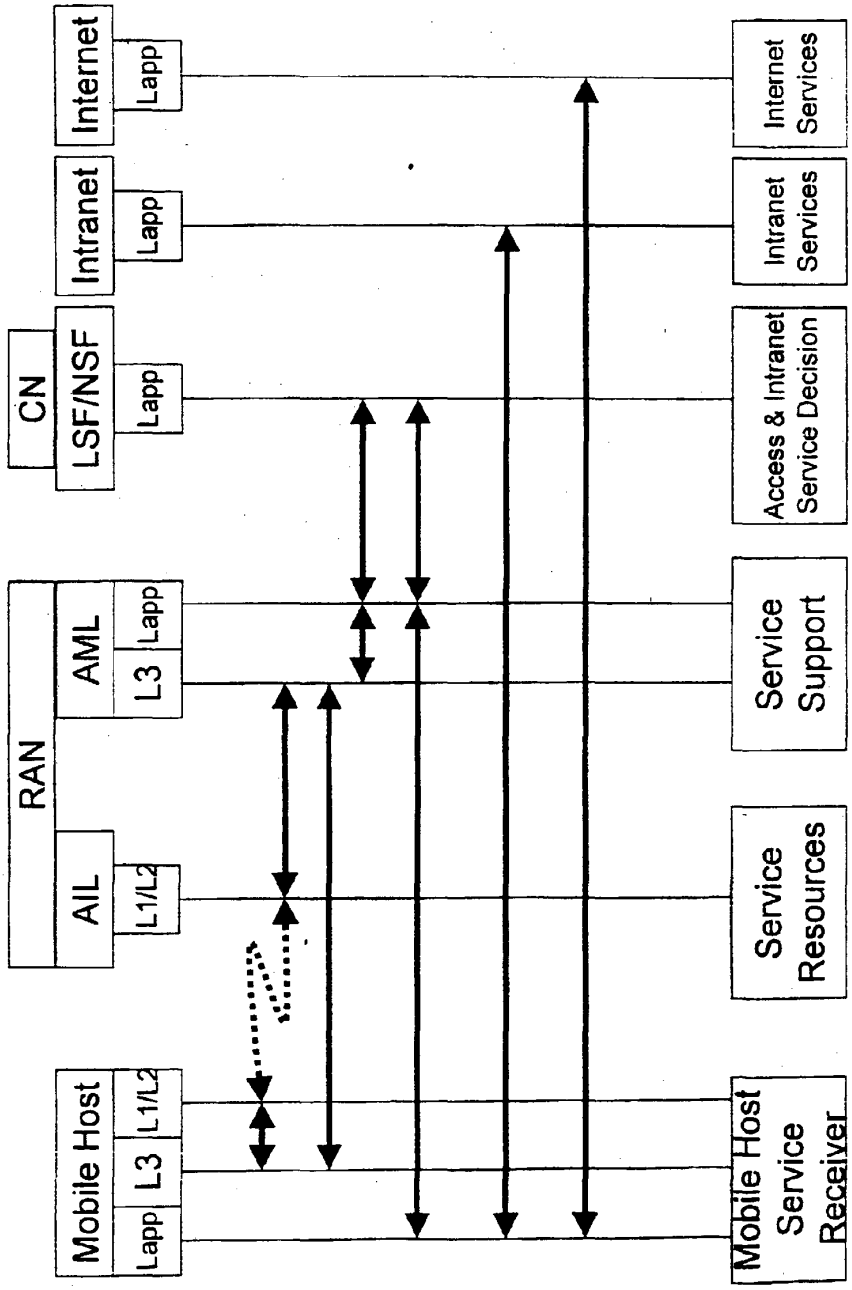


Figure 6

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 778

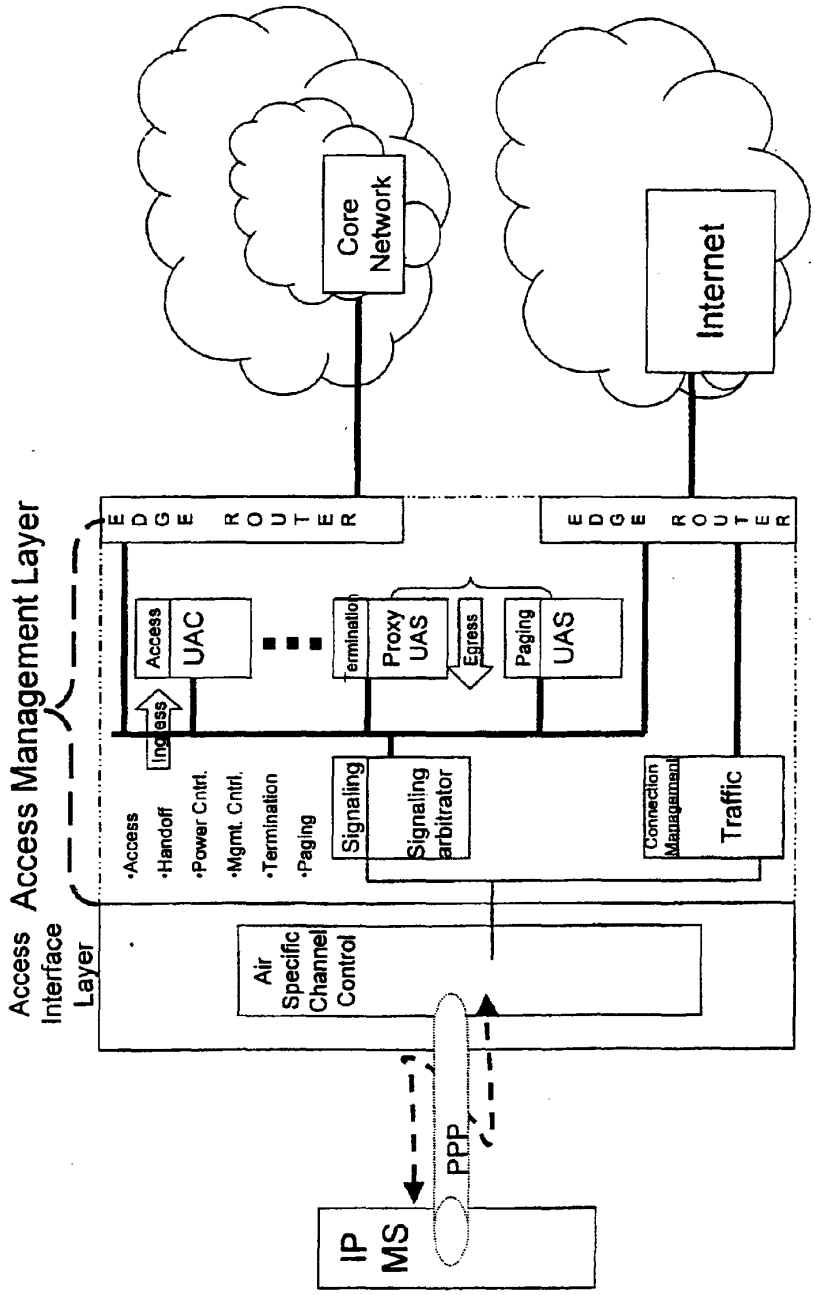


FIGURE 7

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 779

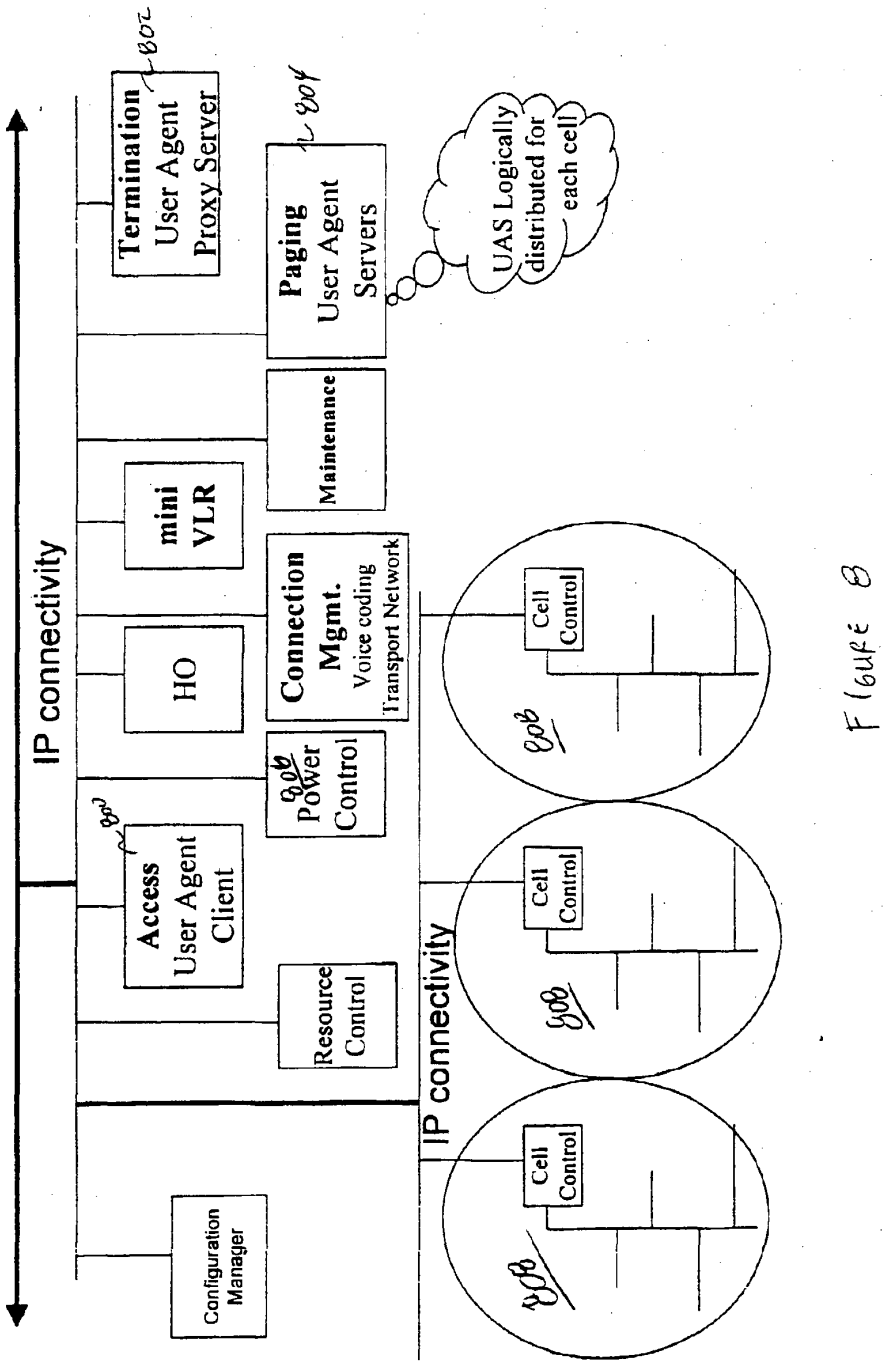


FIGURE 8

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 780

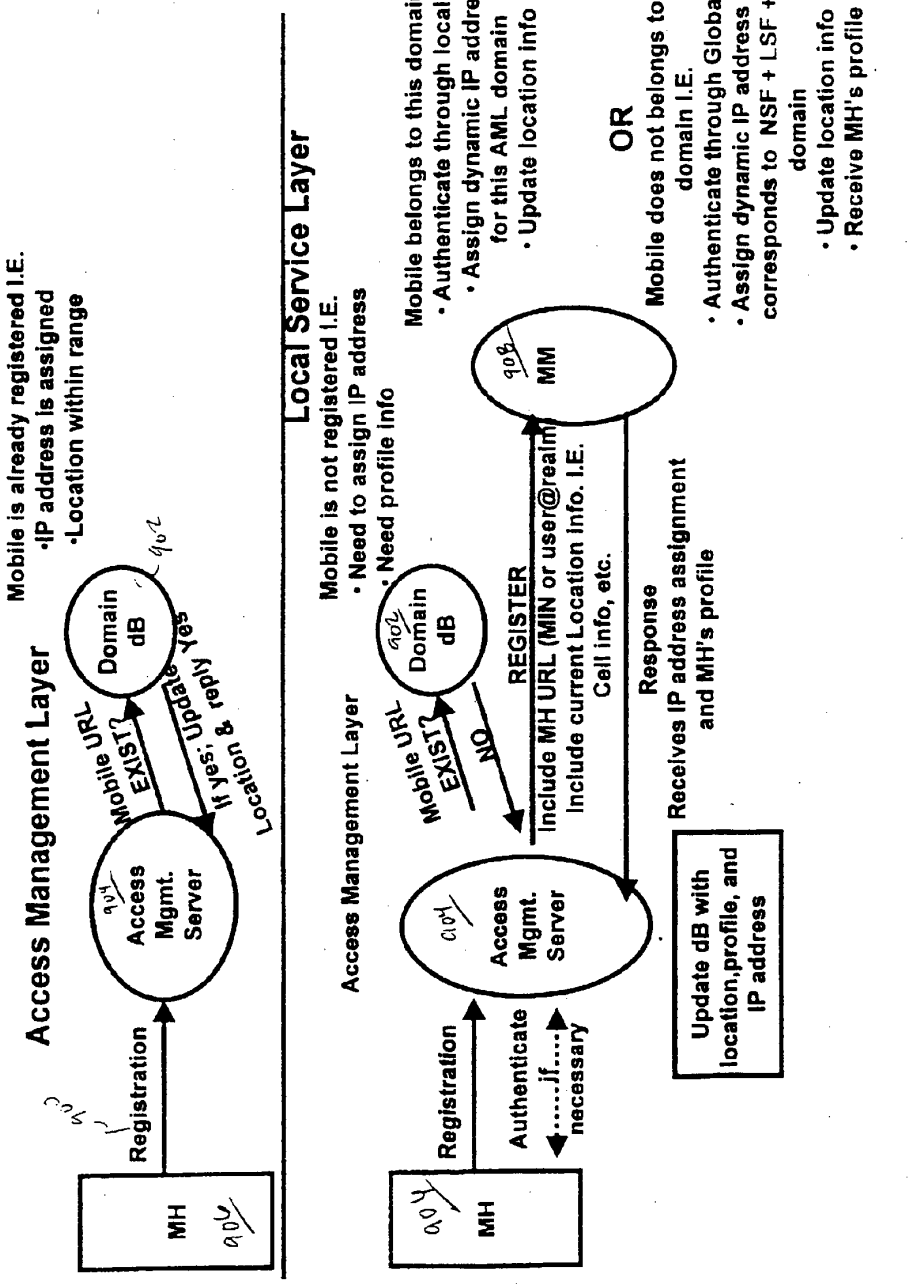


Figure 9

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 781

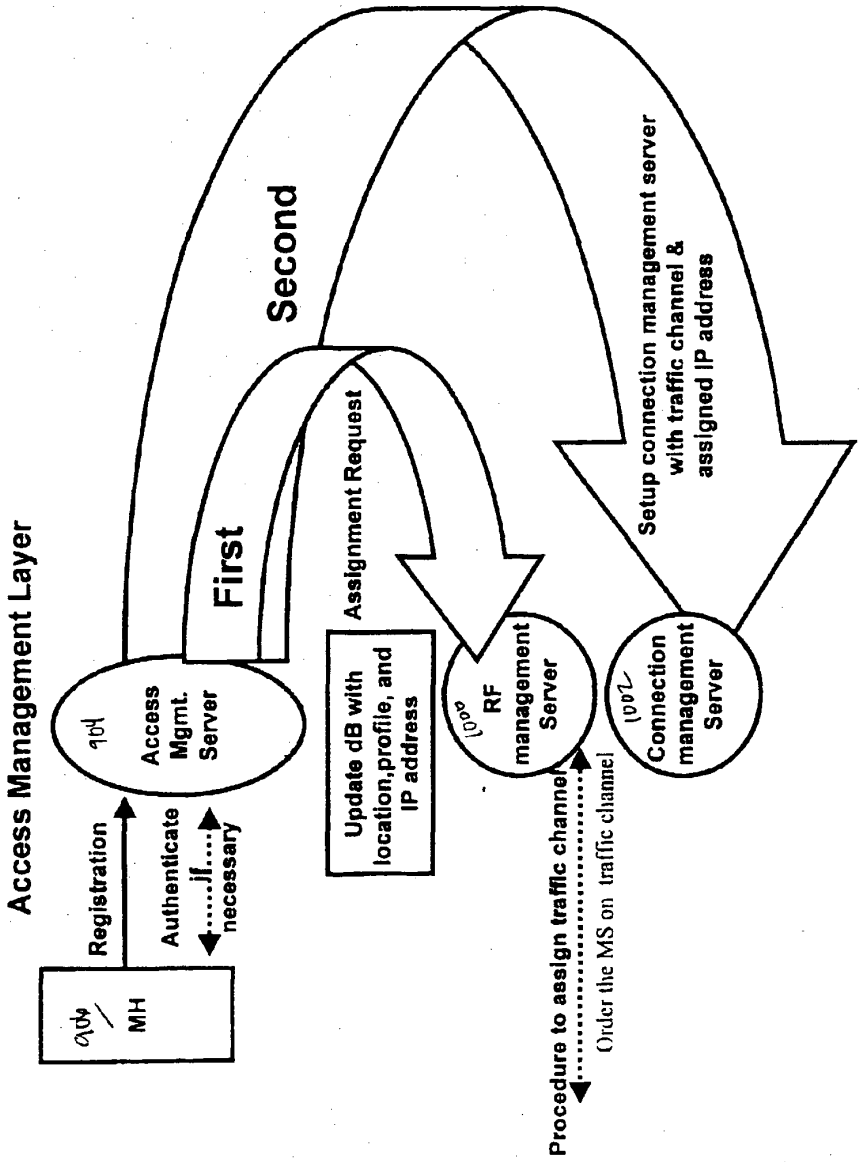


FIGURE 10

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 782

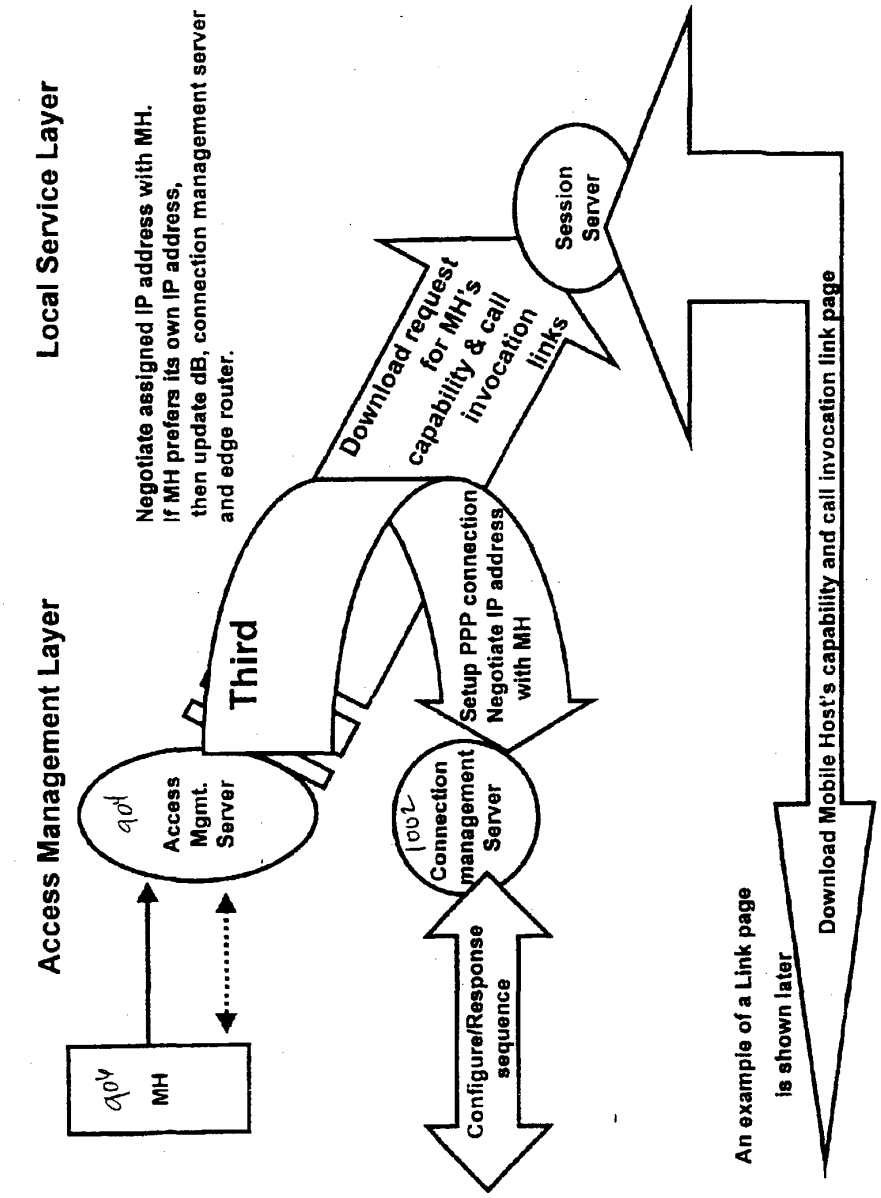


FIGURE 11

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 783

FIGURE 12

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 784

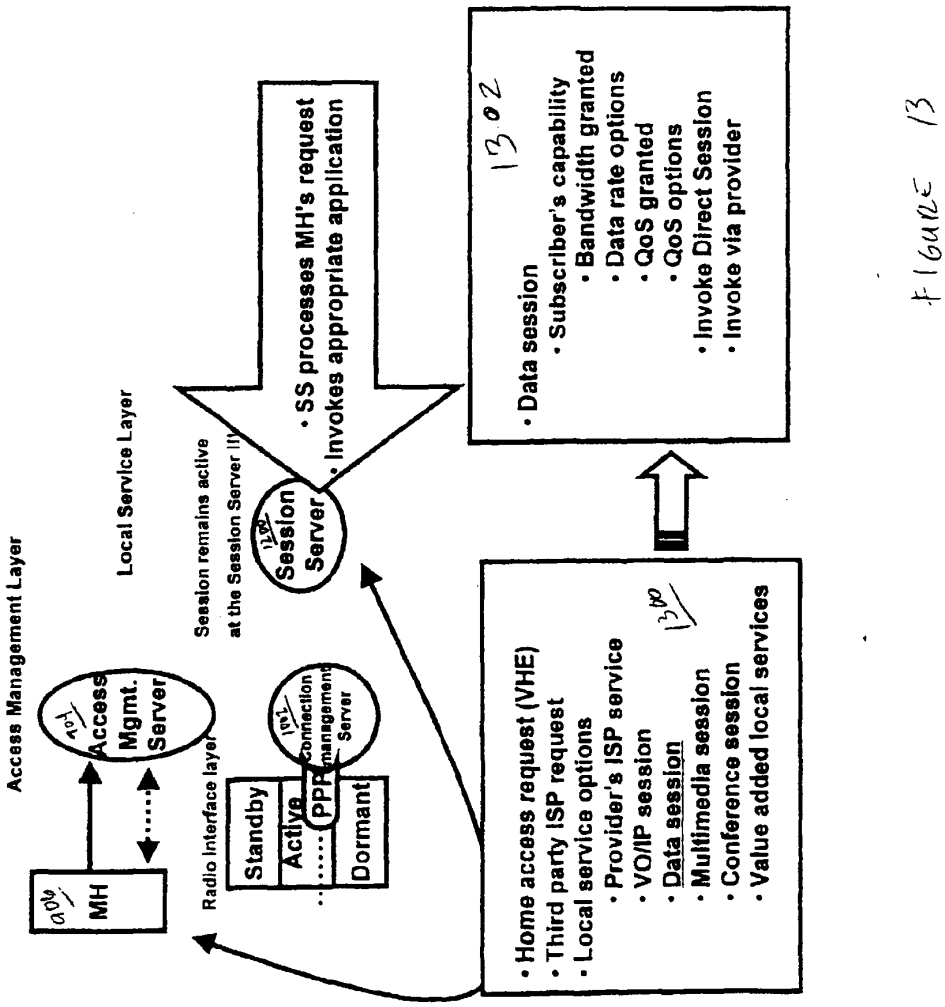


FIGURE 13

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 785

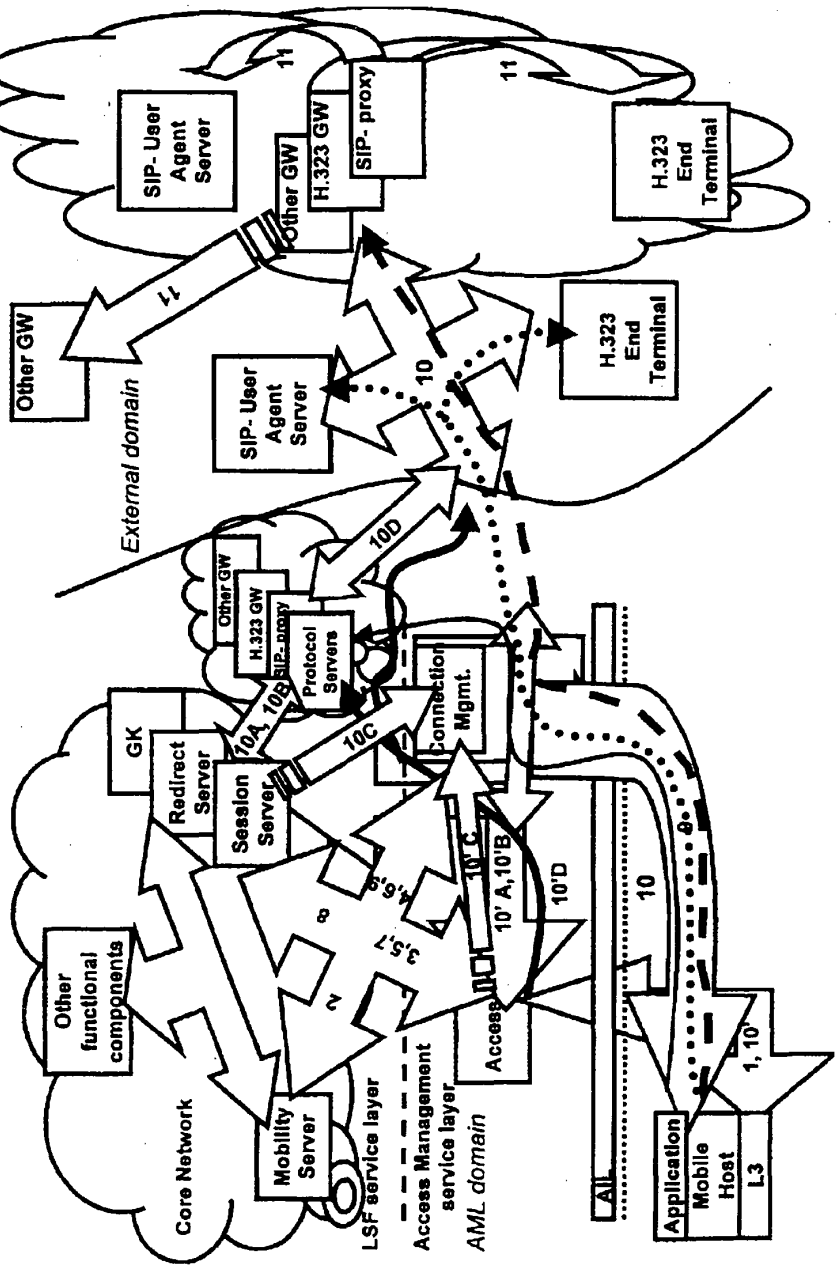


Figure 11

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 786

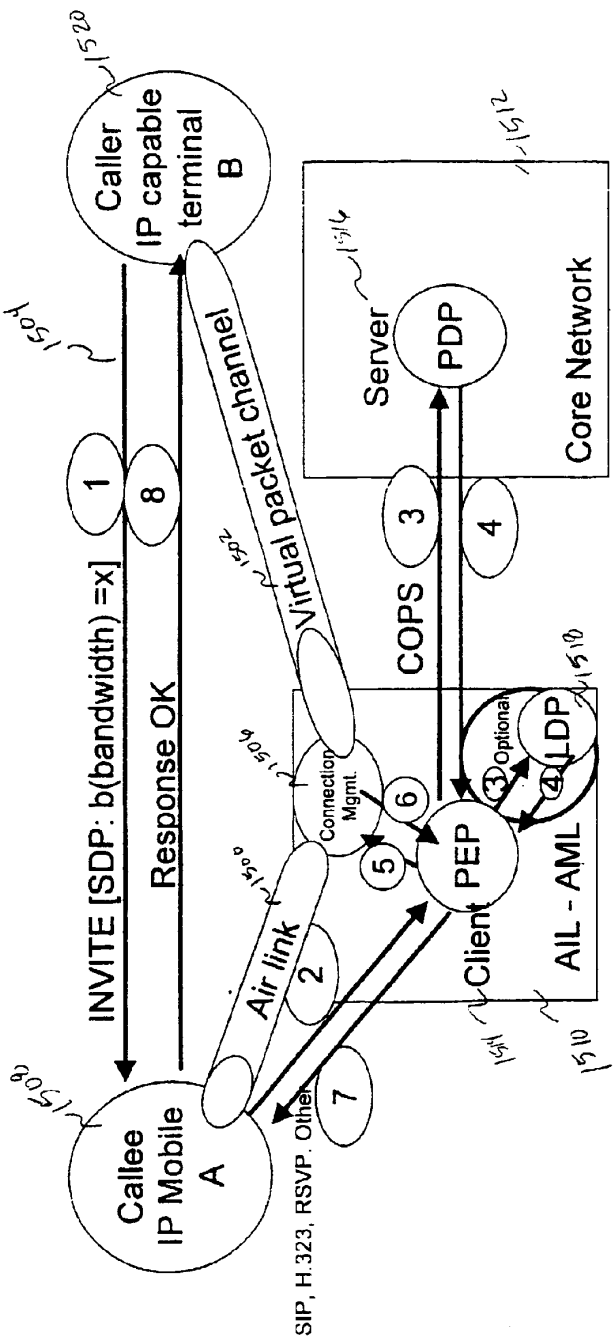


FIGURE 15

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 787

Figure 16

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 788

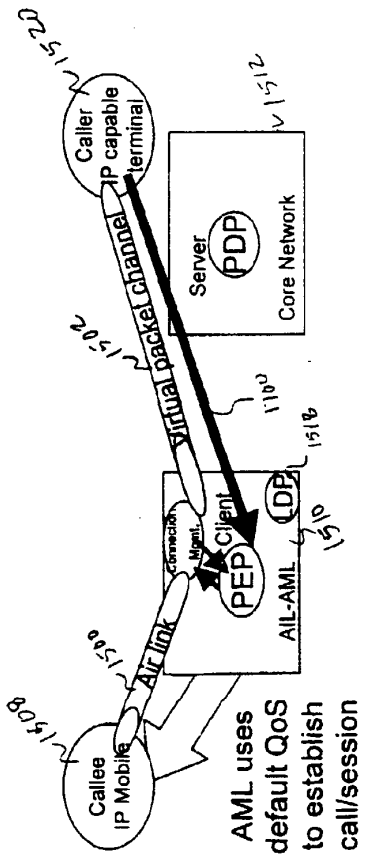


FIGURE 17

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 789

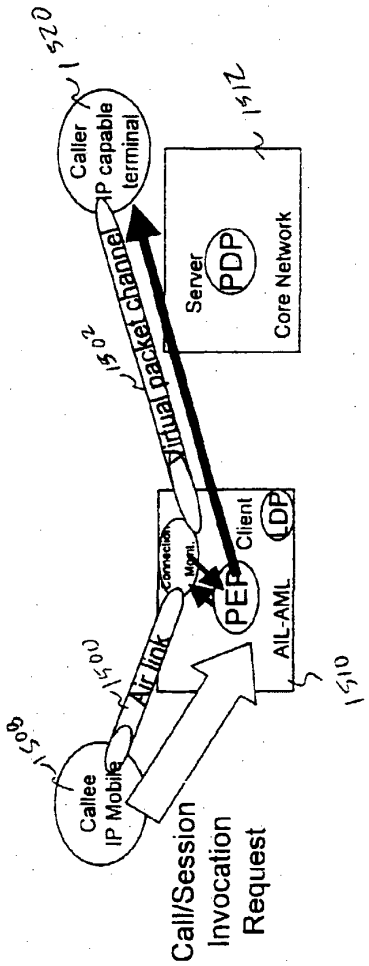


FIGURE 18

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 790

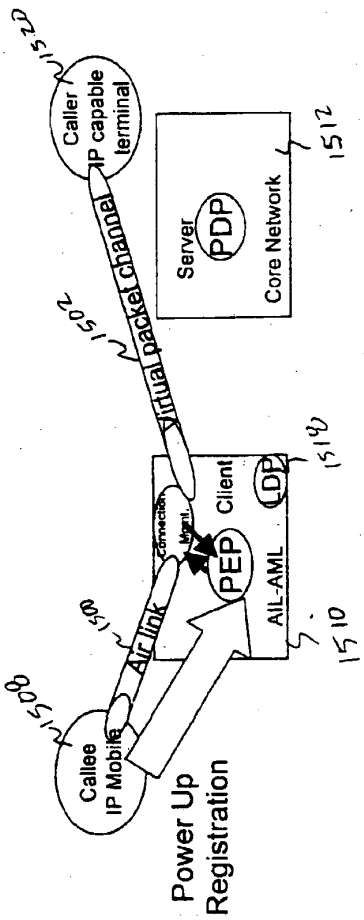
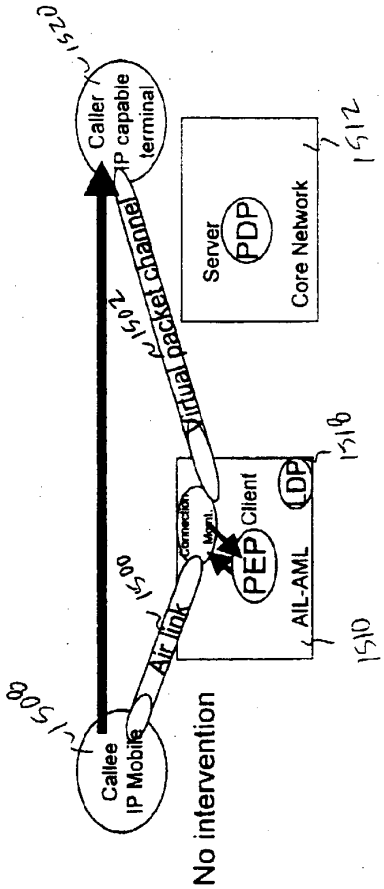


FIGURE 17

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 791

FIGURE 20



BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 792

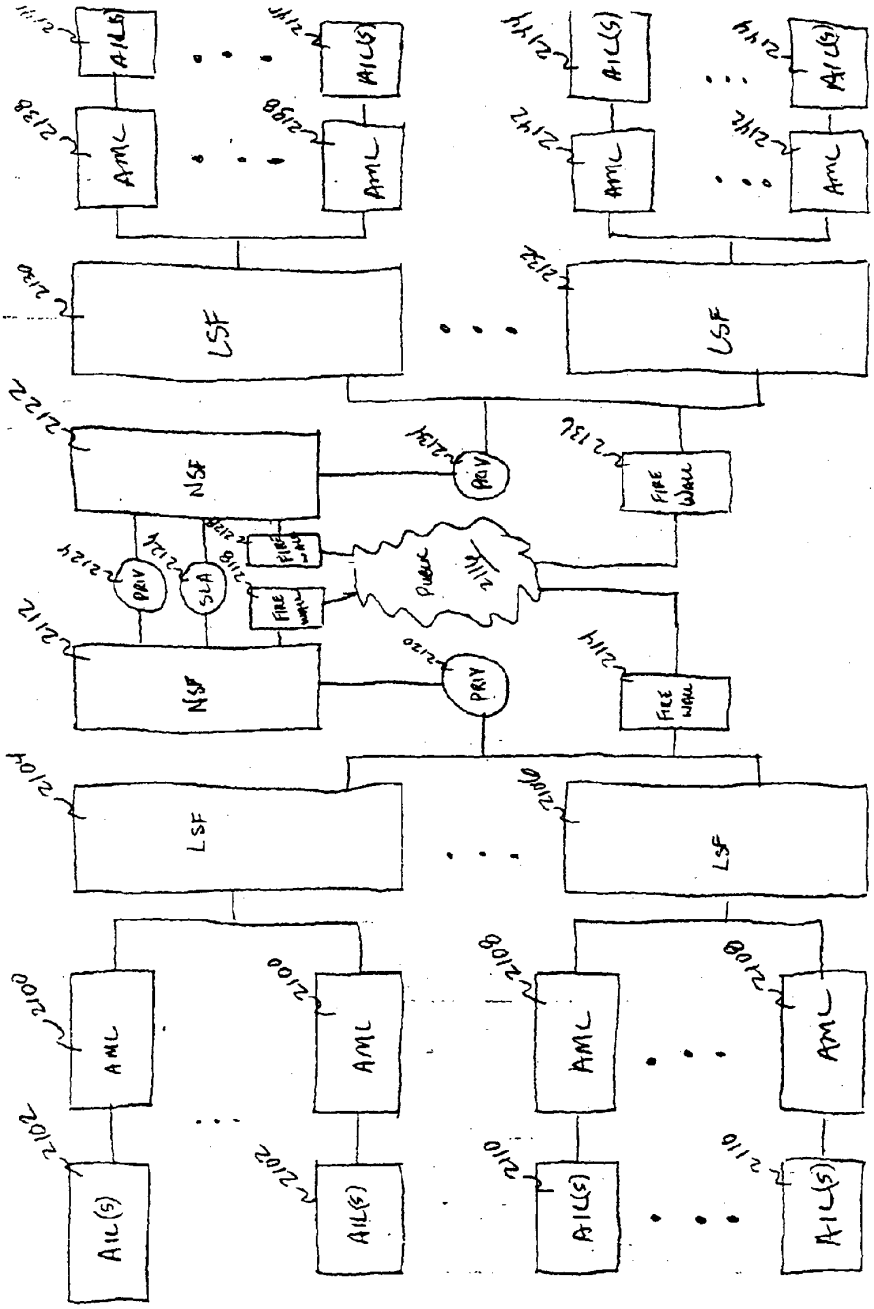


FIGURE 21

BNSDOCID: <EP_____1098490A2_I_>

IPR2025-01572
Apple EX1002 Page 793

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 098 490 A3

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
27.08.2003 Bulletin 2003/35

(43) Date of publication A2:
09.05.2001 Bulletin 2001/19

(21) Application number: **00309735.9**

(22) Date of filing: **03.11.2000**

(51) Int Cl.7: **H04L 29/06**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **05.11.1999 US 434628**

(71) Applicant: **Nortel Networks Limited**
Montreal, Quebec H2Y 3Y4 (CA)

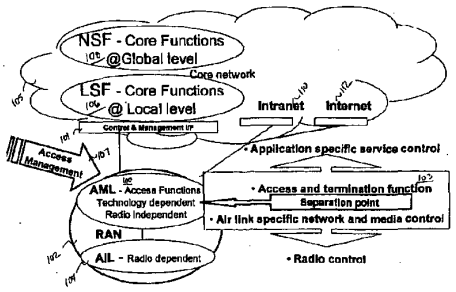
(72) Inventors:
- **Amin, Rajesh B.**
  Desoto, Texas 75115 (US)
- **Hanley, Donald V.**
  McKinney, Texas 75075 (US)
- **Morrow, Glenn C.**
  Plano, Texas 75075 (US)
- **Allahyar, John**
  Dallas, Texas 75252 (US)

(74) Representative: **Mackenzie, Andrew Bryan et al**
Sommerville & Rushton,
45 Grosvenor Road
St Albans, Herts. AL1 3AW (GB)

(54) **An architecture for an IP centric distributed network**

(57) A method and system to for a communications network architecture for an Internet Protocol centric wireless network for a first user to communicate to a destination, the architecture comprising: a network service function layer within the wireless network. The network service function layer can include: a policy management server; an authorization server; a service accounting server; an authentication, authorization and accounting server; an unified directory within a directory server; a security gateway; and a mobility manager. The architecture also includes a local service function layer associated with the network service function layer. The local service function layer can include: an access accounting server; an authentication, authorization and accounting server; a security gateway; a policy enforcement server; a mobility manager; a network management server; and a wireless gateway. The architecture also includes an access management layer associated with the local service function layer. The access management layer can include: a location tracking server; a connection management server; a protocol server; an access management server; a policy enforcement server; a network management server; and a resource management server. The architecture also includes an access interface layer associated with the access management layer. The access interface layer can include: a channel management server; a policy enforcement server; an administration and maintenance server; and a radio frequency server.

FIGURE 1



EP 1 098 490 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 9735

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 99 48310 A (NOKIA TELECOMMUNICATIONS OY ;PUUSKARI MIKKO (FI)) 23 September 1999 (1999-09-23)	1-5, 7-14, 16-23, 26-34, 36-42, 44-50, 52-63, 65-71, 74-83	H04L29/06
Y	* page 1, line 17 - line 24 *	6,15,24, 25,35, 43,51, 64,72,73	
	* page 9, line 2 - line 5 *		
	* page 9, line 27 - page 10, line 23 *		
	* page 11, line 7 - line 30 *		
	* page 12, line 26 - line 29 *		
	* page 14, line 27 - line 29 *		
	* page 19, line 28 - line 35 *		
	* page 22, line 15 - line 20 *		
	* figure 1 *		TECHNICAL FIELDS SEARCHED (Int.Cl.7)

Y	EP 0 910 198 A (LUCENT TECHNOLOGIES INC) 21 April 1999 (1999-04-21)	6,15,24, 25,35, 43,51, 64,72,73	H04L
	* column 2, line 52 - column 3, line 5 *		
	* column 4, line 50 - line 58 *		
	* column 13, line 2 - line 16 *		
	* column 15, line 51 - column 16, line 7 *		
	* column 17, line 40 - line 50 *		
	* column 55, line 5 - line 9 *		

A	EP 0 903 905 A (TOKYO SHIBAURA ELECTRIC CO) 24 March 1999 (1999-03-24)	1-83	
	* the whole document *		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	1 July 2003	HORN, R

CATEGORY OF CITED DOCUMENTS

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

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

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1098490A3_I_>

IPR2025-01572
Apple EX1002 Page 795

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 9735

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.

01-07-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9948310 A	23-09-1999	FI 980617 A	20-09-1999
		AU 2838999 A	11-10-1999
		EP 1064800 A1	03-01-2001
		WO 9948310 A1	23-09-1999
EP 0910198 A	21-04-1999	CA 2249817 A1	14-04-1999
		CA 2249830 A1	14-04-1999
		CA 2249831 A1	14-04-1999
		CA 2249836 A1	14-04-1999
		CA 2249837 A1	14-04-1999
		CA 2249838 A1	14-04-1999
		CA 2249839 A1	14-04-1999
		CA 2249862 A1	14-04-1999
		CA 2249863 A1	14-04-1999
		EP 0912026 A2	28-04-1999
		EP 0910198 A2	21-04-1999
		EP 0917320 A2	19-05-1999
		EP 0917318 A2	19-05-1999
		EP 0912027 A2	28-04-1999
		EP 0912012 A2	28-04-1999
		EP 0917328 A2	19-05-1999
		EP 0918417 A2	26-05-1999
		EP 0912017 A2	28-04-1999
		JP 11289353 A	19-10-1999
		JP 11252183 A	17-09-1999
		JP 11275154 A	08-10-1999
		JP 11275155 A	08-10-1999
		JP 2000022758 A	21-01-2000
		JP 11275156 A	08-10-1999
		JP 11275157 A	08-10-1999
		JP 11284666 A	15-10-1999
		JP 11331276 A	30-11-1999
		US 6577643 B1	10-06-2003
		US 6414950 B1	02-07-2002
		US 6421714 B1	16-07-2002
		US 6377982 B1	23-04-2002
		US 6400722 B1	04-06-2002
		US 2002089958 A1	11-07-2002
		US 6393482 B1	21-05-2002
EP 0903905 A	24-03-1999	JP 11163947 A	18-06-1999
		EP 0903905 A2	24-03-1999
		EP 0903906 A2	24-03-1999
		JP 11163946 A	18-06-1999
		US 6418128 B1	09-07-2002
		US 6272148 B1	07-08-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____1098490A3_I_>

IPR2025-01572
Apple EX1002 Page 796

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 9735

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.

01-07-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0903905 A		US 2002186680 A1	12-12-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____1098490A3_I_>

IPR2025-01572
Apple EX1002 Page 797

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2007 (15.11.2007)

PCT

(10) International Publication Number
WO 2007/129180 A2

(51) International Patent Classification:
H04B 7/005 (2006.01)

(21) International Application Number:
PCT/IB2007/001120

(22) International Filing Date: 30 April 2007 (30.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/797,943 5 May 2006 (05.05.2006) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, Texas 75039 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KAIKKONEN, Jorma** [FI/FI]; Taskilantie 27 D 15, FIN-90580 Oulu (FI). **VIMPARI, Anna-Mari** [FI/FI]; Kummelintie 9, FIN-90520 Oulu (FI). **HINTZ-MADSEN, Mads** [DK/FI]; Luokkikuja 6, FIN-90310 Oulu (FI).

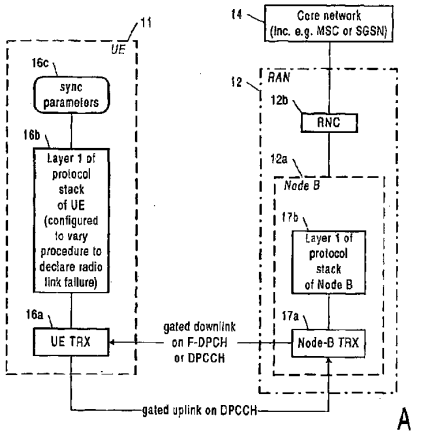
(74) Agents: **MAGUIRE, Francis, J.** et al.; Ware, Fressola, Van Der Sluys & Adolphson LLP, 755 Main Street, P.O. Box 224, Monroe, Connecticut 06468 (US).

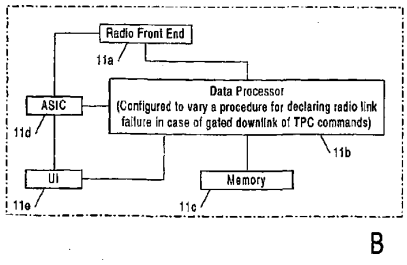
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, 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.

(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),

[Continued on next page]

(54) Title: ENHANCED UE OUT-OF-SYNC BEHAVIOR WITH GATED UPLINK DPCCH OR GATED DOWNLINK F-DPCH OR DPCCH TRANSMISSION





(57) Abstract: A method and corresponding equipment by which a wireless terminal communicatively coupled to a radio access network adapts to gating in respect to a downlink signal from a radio access network carrying power control commands (e.g. the F-DPCH of UTRAN with WCDMA), including gating by the radio access network of either just the power control commands or the channel itself, or gating of reception of the power control commands by the user equipment. The adaptation can include changing values of parameters used in determining when the wireless terminal declares a radio link failure, or instead only changing the procedures used to determine whether a parameter value has been achieved and thus only effectively changing the parameter values (or one or more of the parameters can be actually and effectively changed).

WO 2007/129180 A2

IPR2025-01572
Apple EX1002 Page 798

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).

Published:

— *without international search report and to be republished upon receipt of that report*

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.

BNSDOCID: <WO_____2007129180A2_I_>

ENHANCED UE OUT-OF-SYNC BEHAVIOR WITH GATED UPLINK DPCCH OR GATED DOWNLINK F-DPCH OR DPCCH TRANSMISSION

CROSS REFERENCE TO RELATED APPLICATION

Reference is made to and priority claimed from U.S. provisional application Ser. No. 60/797,943 filed 5 May 2006.

BACKGROUND OF THE INVENTION

1. *Technical Field*

The present invention pertains to the field of wireless communications. More particularly, the present invention pertains to procedures to be followed by wireless terminals in case of gating of transmit power by the wireless terminals.

2. *Discussion of related art*

In some wireless communications systems, in particular UMTS (Universal Mobile Telecommunications System) using WCDMA (Wideband Code Division Multiple Access) for the air interface of its UTRAN (UMTS terrestrial radio access network), in order to save power a UE (user equipment) wireless communication terminal could turn its transmit power on and off, i.e. it could *gate* its transmit power according to a gating pattern (among other factors), i.e. according (at least in part) to a duty cycle having an on period and an off period. Using a UTRAN with WCDMA as an example, a UE sends data and/or control information (such as pilot bits) to a Node-B of the UTRAN, and the Node-B then estimates the UE uplink quality based on the control information, and commands the UE to change its transmit power accordingly. If a UE were to use transmit power gating, there would then be periods of time in which no control information would be transmitted, and correspondingly, there could be periods of time in which no power change commands would be issued by the Node-B, or periods of time in

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 800

which if the Node-B were to issue power change commands, the commands would be based on unreliable quality information (signal to interference ratio measurements, for example) because of no control bits having been transmitted for the period of time in which the quality measurements are made (taking into account the time it takes for a transmission from the UE to reach the Node-B).

At present, there are procedures according to which a UE is to declare a radio link failure based on a predetermined threshold for minimum quality of the signal from the Node-B, and a predetermined value for a number of consecutive below threshold quality indications. These procedures and the predetermined threshold and number of below minimum quality indications assume continuous transmit power by the UE. But if a UE were to gate its uplink, then because the Node-B would in effect follow and gate its downlink (because of having no control information to estimate the uplink quality from when the UE is not transmitting), and because the UE uses the downlink as a basis for estimating the quality of the radio link, the UE could declare a radio link failure when in fact there would be no such failure. The apparent inability to "hear" the Node-B for a period of time would be due simply to the Node-B not transmitting during that period of time, not because of poor radio link quality.

What is needed, therefore, is a way to adapt the procedure for declaring a radio link failure, and also related procedures, in case of a UE gating its uplink.

UTRAN with WCDMA as the radio technology is a particular example of the need for a new procedure for declaring a radio link failure. First consider the need for gating by a UE. When no dedicated channels (DCHs)--and thus, no dedicated physical data channels (DPDCHs) (which carry payload as well as high-level signalling)--have been configured in the uplink

BNSDOCID: <WO____2007129180A2_|_>

IPR2025-01572
Apple EX1002 Page 801

(UL), all data is transmitted on the enhanced data channel (E-DCH), which is mapped to the enhanced dedicated physical data channel (E-DPDCH). Control signalling associated with E-DCH is transmitted on E-DPCCH. E-DPDCH and E-DPCCH are discontinuous, i.e. they are transmitted only when there is data to be transmitted and the transmission has been granted by the network. For an E-DCH transmission, a grant is needed: a non-scheduled grant for non-scheduled MAC-d (media access control-d) flows and a serving grant (and an allowed, active HARQ process) for scheduled transmissions.

The UL DPCCH carries control information generated at Layer-1 (i.e. the physical layer of the protocol stack). The layer-1 control information consists of e.g. known pilot bits for supporting channel estimation for coherent detection, for use in the Node-B determining transmit power control (TPC) commands to downlink (DL) on DPCH or on Fractional-DPCH (F-DPCH), feedback information (FBI), and an optional transport format combination indicator (TFCI).

UL DPCCH is continuously transmitted (even if there is no data to transmit for awhile), and there is one UL DPCCH for each radio link. Continuous transmission is acceptable with circuit-switched services, which typically send continuously. For bursty packet services, however, continuous DPCCH transmission is less desirable because it has substantial overhead.

The uplink capacity can be increased by decreasing the control overhead. One possibility for decreasing control overhead is UL DPCCH gating, i.e., not transmitting DPCCH all the time. A pattern could (at least in part) define the DPCCH transmission time periods and/or DPCCH may depend (also) on E-DCH and HS-DPCCH transmission times. (Other rules may in effect supercede the pattern so that from time to time the UE may uplink during what would ordinarily be an off-period/gap

BNSDOCID: <WO_____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 802

in the transmission, with the net result being irregular transmission, i.e. not strictly according to a pattern.) Gating can provide UE power saving and so longer battery life, depending on the duty cycle, i.e. the length of on period for DPCCH compared to the off period. Also, interference with other UEs could be reduced, and thus network capacity could be increased.

F-DPCH carries TPC command bits to a UE determined by the Node-B serving the UE, based on data and/or control information uplinked by the UE on DPCCH. F-DPCH is currently transmitted every time slot, independently of the data or control transmission activity by the UE, i.e. independent of whether the UE gates the DPCCH. However, in case of UL DPCCH gating by the UE so that an UL DPCCH time slot does not contain and data and/or control transmission by the UE (i.e. because the UE does not transmit during that UL DPCCH time slot on account of its gating), the Node-B cannot derive a sensible power control command corresponding to the time slot, to transmit on F-DPCH. Thus, if UL DPCCH is to be gated, F-DPCH and/or DL DPCCH could also be gated and/or discontinuously received. Discontinuous DL transmission decreases downlink interference and corresponding discontinuous reception by the UE improves UE battery consumption.

With respect to power control commands issued by the serving Node-B, a UE is considered out-of-sync (not synchronized) if the DL DPCCH quality or the quality of the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the previous 160 ms period is worse than a threshold Q_{out} defined (implicitly) by tests in 3GPP TS 25.101. A UE is considered in-sync (synchronized) if the UE estimates the quality of the DL DPCCH or the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the previous

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 803

160 ms period to be better than a threshold Q_{in} also defined (implicitly) by tests in 3GPP TS 25.101.

According to 3GPP TS 25.101, if a UE estimates the DPCCH quality or the quality of the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the last 160 ms period to be worse than the threshold Q_{out}, the UE is to turn its power off. On the other hand, if a UE estimates the DPCCH quality or the quality of the TPC fields of the F-DPCH frame received from the serving HS-DSCH cell over the last 160 ms period to be better than the threshold Q_{in}, the UE is to turn its power on. A UE is to determine that radio link failure has occurred if after some number N313 of consecutive out-of-syncs have been indicated (N313 being the label of a parameter whose value is the number), less than some number N315 of successive in-syncs are indicated before some number T313 of time periods expires (where the counting toward the number T313 is starting from when the N313 consecutive out-of-syncs are indicated).

Disclosure of Invention

The invention provides a method for use by a user equipment wireless communication terminal, comprising: determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure. To actually vary a parameter, the value of the parameter would be changed. To only effectively vary a parameter, a procedure using the parameter is changed but the value of the parameter is not changed (so that the same parameter value then has a different effect).

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 804

Corresponding equipment, including computer program products and application specific integrated circuits are also provided. In addition, wireless terminals are provided including such equipment and so operative according to methods provided by the invention. Also, a wireless communication system including elements communicatively coupled to such wireless terminals are also provided.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects, features and advantages of the invention will become apparent from a consideration of the subsequent detailed description presented in connection with accompanying drawings, in which:

Figure 1A is a block diagram/ flow diagram of a UE and a Node-B communicatively coupled via a radio link including a gated uplink channel and a gated downlink channel, and showing parameters stored in the UE for use in (among other things) determining when to declare a radio link failure.

Figure 1B is a reduced block diagram (only portions relevant to the invention being shown) of the UE terminal or the Node B of Figure 1A.

Figure 2 is a block diagram showing a layer one (physical layer) of a protocol stack implemented in the UE receiving as inputs information indicating the gated downlink, and also the sync parameter values in case of no downlink gating, and providing changed sync parameters.

Figure 3 is a flow chart of the operation of a UE, according to the invention.

Figure 4 is a flow chart of the operation of a Node, B according to the invention.

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 805

BEST MODE FOR CARRYING OUT THE INVENTION

The invention provides a method by which a UE, communicatively coupled to a Node-B of a UTRAN (UMTS radio access network) (or coupled to a corresponding entity of a radio access network on another cellular technology), adapts to gating (so as to perform what is sometimes called discontinuous transmission) of a downlink channel (F-DPCH or DPCCH) carrying power control commands from the Node-B. As explained above, such gating of the downlink can be the direct result of gating of the uplink by the UE, or can be at least associated with such gating, and the downlink gating is presumed known or knowable to the UE (as a result of monitoring/ measurements or other mechanism not the subject of the invention). As also explained above, the UE is required by standards to turn its power off in case of a number of consecutive out-of-sync indications, each corresponding to a determination that a quality metric for receiving control commands from the Node-B is below a threshold Q_{out}. Without adapting to such gating, the UE could turn its power off more than is desirable because of out-of-sync indications due simply to the Node-B not transmitting for a period of time--the off period of an on/off duty cycle. As indicated above, what is needed therefore, is a way to adapt the procedure for declaring a radio link failure, and also related procedures, in case of a UE gating its uplink.

In case of gating, different options exist for how the out-of-synch criterion could be determined. In general, according to the invention, to accommodate gating by the Node-B, the UE actually and/or effectively varies one or more parameter values used to determine when to declare a radio link failure based on the downlink gating. To actually vary a parameter, the value of the parameter is changed. To effectively vary a parameter, a procedure using the parameter

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 806

is changed but the value of the parameter used in the procedure is not. For example, a procedure could require a number N of occurrences of an event in a time T. To actually vary N, the value of N would be changed, but not (necessarily) the value of T. (Alternatively, the value of T could be actually changed.) To effectively vary N, how T is measured could be changed. (This can also be viewed as effectively changing the value of T.) For example, the procedure could be changed so that off-period of a duty cycle does not count in measuring T.

Now in a first option for how the out-of-synch criterion could be determined, the Q_{out} and Q_{in} thresholds and the measurement window (the 160 ms time period) could be kept unchanged, and values for the parameters N313, T313 and N315, could be signaled to a UE to achieve the desired behavior for the downlink gated transmission. However, this has as a disadvantage lowered reliability of Q_{in} or Q_{out} due to a lower number of samples. In addition, the parameters are currently broadcast, and so they would need to be separately set for each user having a different gated transmission.

In a second option, the thresholds and parameters could be kept unchanged, but the measurement window could be increased (from 160 ms), or instead only effectively increased by counting only time increments when according to the gated transmission by the Node-B there is an actual downlink transmission. With both approaches--increasing the window or only changing how time is counted as contributing to the window--the measurement window could be set so that the number of evaluated samples (in terms of TPC commands) would be kept constant. This way the reliability of Q_{in} or Q_{out} could be improved.

In a third option, the option provided by the invention in at least some embodiments, the N313, T313 and N315

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 807

parameter values would be broadcast by the network as before (and so known to all UEs served by the Node-B broadcasting the parameters). However, a UE would autonomously adjust one or more of the broadcast values for the N313, T313 and/or N315 parameters based on an on period and an off period of a gated transmission having an on/off duty cycle and associated with the transmission of the power control commands on the downlink channel of the radio access network, based on a predetermined methodology. In some other embodiments, the UE could adjust the values it used for the thresholds Q_{out} and Q_{in}.

In case of a UE changing the values it uses for one or more of the N313, T313 and N315 parameters, the methodology could, for example, increase the value of the T313 value and so lengthen the time before a radio link failure is declared (and perhaps prevent declaring a radio link failure because of allowing more time to receive an in-sync indication after N313 out-of-sync indications). For example, the T313 parameter would be increased by the percentage of time the Node-B is not transmitting compared to the total time. Alternatively, the methodology could increase the number N313 to require a greater number of out-of-sync indications, and again for example, in direct proportion to the off period of the duty cycle compared to the whole period of the duty cycle. (This alternative starts the T313 and N315 usage and thus has the greatest impact.) In still another alternative, the methodology could decrease the number N315 and so decrease the number of consecutive in-sync indications (before T313 units of time has expired) required to prevent a declaration of radio link failure (after N313 consecutive out-of-sync indications have been observed).

The invention also encompasses changing not just one of the N313, T313 and N315 parameters, but any combination of these parameters. Also, instead of changing a parameter value in direct proportion to the length of the off-period of the

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 808

gated transmission (i.e. the off-period of the duty cycle of the UE transmitter), the parameter values could be changed in some other proportion, i.e. in a non-linear way.

As an alternative to changing the values of the N313, T313 and N315 parameters, the UE could change how it counts consecutive out-of-sync indications, and how it counts consecutive in-sync indications, and/or how it measures the time period corresponding to T313. The UE could, for example, only count as a consecutive out-of-sync indication an indication of out-of-sync occurring in a time when the Node-B gated transmission is in an on-period, i.e. when the Node-B is known by the UE to be transmitting. Similarly for the counting up to N315 in-sync indications, and similarly for measuring time after N313 consecutive out-of-sync indications (i.e. time would be measured only when the Node-B is known to be transmitting). Thus, the UE could only *effectively* change one or more of the N313, T313 and N315 parameter values, by changing how the UE determines whether a condition(s) corresponding to the one or more parameter values has occurred, e.g. changing the procedure used to monitor out-of-sync indications so as to count as a consecutive out-of-sync indication such an indication only if the out-of-sync indication occurs during the on period of the on/off duty cycle (and only if there has not been an in-sync indication anytime between the most recent previous out-of-sync indication occurring during an on period).

In order to vary (one or more of) the N313, T313 and N315 parameters (actually or just effectively), the UE must learn/ determine the on period and the off period of the on/off duty cycle used by the Node-B of the radio access network in gating the downlink channel conveying the power control commands. One way for the UE to determine the on and off periods of the duty cycle is by assuming that they are the same as the on and off periods of the duty cycle used by the UE in gating its

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 809

uplink (on DPCCH), and so equating the downlink gated transmission by the Node-B to the uplink gated transmission of the UE. Another way is to monitor the downlink, observing the pattern of variation in received power on the gated downlink channel (for example, the F-DPCH in case of WCDMA and UTRAN), and equating the off period of the gated downlink pattern to the observed period of low received power, and equating the on period to the observed period of higher low received power. Another way is for the UE to receive via signaling from the Node-B information indicating the gated transmission used by the Node-B, and to determine from the signaling the on period and the off period of a duty cycle.

As mentioned, a UE could also change one or more of the values it uses for the thresholds Q_{out} and/or Q_{in}. This could be as an alternative to changing one or more of the N313, T313 and N315 parameters, or in addition. A UE could autonomously adjust the values it uses for the thresholds Q_{out} and/or Q_{in}, or it could select the values of the thresholds from a predefined set (in determining when out-of-sync or in-sync occurs and through out-of-sync / in-sync indications determining when a radio link failure is deemed to have occurred).

Instead of gating the downlink channel (and in particular, F-DPCH or DPCCH), the downlink channel could be continuously transmitted but discontinuously power controlled due to uplink gating, i.e. power control commands could be sent only in downlink time slots corresponding to uplink time slots when the UE is transmitting. Alternatively, the downlink channel (F-DPCH or DPCCH) could be continuously transmitted, but discontinuously received by the UE, in order to improve UE power consumption. Discontinuous power control potentially degrades performance during uplink transmission gaps and right after the gaps. Therefore methods could be applied similar to those described above and below (for use in case of a gated downlink channel) that treat downlink

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 810

transmission during periods corresponding to an uplink transmission gap similarly to downlink off periods (of a gated downlink). Discontinuous reception is in effect the same as a gated downlink channel from the standpoint of F-DPCH usage in the UE and performance.

Referring now to Figure 1A, a UE 11 is shown communicatively coupled to a Node-B 12a of a UTRAN 12, via a radio link having an uplink and a downlink, where the downlink is gated according to a gated transmission, and the uplink is also gated (and as explained above, may cause the gating of the downlink). As illustrated, the UTRAN also includes a Radio Network Controller (RNC) 12b, for controlling the Node-B in at least some respects, and for coupling the Node-B to a Core Network 14 (and hence ultimately to other communication terminals, not shown). The UE is shown as including a UE transceiver (TRX) 16a rigged for radio communication with a corresponding Node-B TRX 17a. The UE is shown as also including a Protocol Stack Layer-1 16b that operates the UE TRX 16a, and the Node-B is shown as including a peer Protocol Stack Layer-1 17b. The UE is shown as also including a data store 16c for holding values of the various parameters and/ or thresholds used in different embodiments of the invention, called here the sync parameters.

Figure 1B shows some components of the UE 11 of Figure 1A from a different perspective. The UE is shown as including a suitable radio front end 11a (including a wireless transceiver, not shown) coupled to a data processor 11b that in turn is coupled to a (volatile and/or non-volatile) memory structure 11c. The data processor can be for example a microprocessor, i.e. a programmable digital electronic component that incorporates the functions of a central processing unit on a single semiconducting integrated circuit. The radio front end may include a digital signal processor (not shown), or the data processor 11b may provide digital

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 811

signal processing in respect to signals transmitted or received by the wireless terminal. The memory structure 11c stores program code that is executable by the processor 11b, including program code that is provided to implement all or part of the invention. The UE 11, as shown, can also include one or more application specific integrated circuits 11d, for providing some or all of the functionality of the UE, as an alternative to providing the functionality via stored instructions executed by the processor. Finally, the UE 11, as shown, includes a user interface (UI) 11e (usually including, among other things, a display, a keypad, a microphone, and a speaker), coupled to the data processor and possibly also to one or more of the one or more ASICs. The UE TRX 16a of Figure 1A is a component of the radio front end 11a. The UE Protocol Stack Layer-1 16b of Figure 1A can be implemented so as to include one or more ASICs 11d, and/or program code stored in the memory structure 11c executable by the data processor 11b, and/or one or more components of the radio front end 11a.

Although not illustrated in the drawings, it will be appreciated that each Node-B 12a also includes a radio front end and a data processor and a memory structure and may include one or more ASICs coupled as shown in Figure 1B, and the RNC 12b also includes a data processor and a memory structure and possibly one or more ASICs.

In general, the various embodiments of the UE 11 can include, but are not limited to, cellular telephones, personal digital assistants (PDAs) having wireless communication capabilities, portable computers having wireless communication capabilities, image capture devices such as digital cameras having wireless communication capabilities, gaming devices having wireless communication capabilities, music storage and playback appliances having wireless communication capabilities, Internet appliances permitting wireless Internet

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 812

access and browsing, as well as portable units or terminals that incorporate combinations of such functions.

Referring now also to Figures 2 and 3, in a first step 31, the UE determines that the downlink is gated, and then in a next step 32 adjusts values of one or more of the sync parameters it uses (actually or only effectively, as described above) compared to values used in case of no gating of the downlink. The term "sync parameter" is used here to indicate any one or more of the N and T parameters (N313, T313 and N315), and/ or any one or more of the thresholds (Q_{out} and Q_{in}). The adjustment is based on the downlink gated transmission. (As explained above, the adjustment may be based on, or may be proportional to, the off period of the on/off duty cycle of the gated transmission.) In Figure 2, the UE is shown (optionally) obtaining original values of the procedures and then storing the changed sync parameters (i.e. their values) in a data store of the UE for use for example in determining when to declare a radio link failure (or otherwise responding to out-of-sync or in-sync indications). As indicated in Figures 1 and 2, the functionality for changing the sync parameters can reside in the layer one (physical layer) implementation (in hardware or software) of the UE protocol stack.

Referring now to Figure 4, the Node-B is indicated there as operative according to a first step 41 in which the Node-B determines that the UE is gating its uplink. The Node-B can make such a determination by for example monitoring the power received on the uplink channel in case of a dedicated channel. In a next step 42, the Node-B gates its downlink to correspond to the uplink gating by the UE. For example, as explained above, the Node-B can simply respond to power change requests actually received (during an on period of the UE uplink gated transmission), and even turn off its receiver during the off period of the UE uplink.

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 813

The functionality described above as provided by the invention can be implemented as software modules stored in a non-volatile memory of a device such as a mobile station, and executed as needed by the device (or more specifically, an operating system of the device) copying all or part of the software into executable RAM (random access memory). Alternatively, the logic provided by such software can also be provided by an ASIC (application specific integrated circuit). In case of a software implementation, the invention provided as a computer program product including a computer readable storage structure embodying computer program code--i.e. the software--thereon for execution by a computer processor.

It is to be understood that the above-described arrangements are only illustrative of the application of the principles of the present invention. Numerous modifications and alternative arrangements may be devised by those skilled in the art without departing from the scope of the present invention, and the appended claims are intended to cover such modifications and arrangements.

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 814

What is claimed is:

1. A method for use by a user equipment wireless communication terminal, comprising:

determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or one or more parameter values used in the procedure.

2. A method as in claim 1, wherein the gated transmission corresponds to a gating of transmission power or a gating of only the power control commands or a gating of reception of the power control commands by the UE.

3. A method as in claim 1, wherein the procedure is varied by changing how to measure a parameter value used by the procedure.

4. A method as in claim 3, wherein the change in the procedure is to count occurrences of events corresponding to the parameter value only if the events occur during one or another of the on periods of the gated transmission, instead of counting occurrences of such events regardless of when the events occur.

5. A method as in claim 3, wherein the change in the procedure is to count occurrences of events corresponding to the parameter for a period of time longer than in case of no gating.

6. A method as in claim 5, wherein the procedure used to measure when the parameter value is changed includes evaluating

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 815

power change commands received during a time window, and wherein the change in the procedure is to evaluate power change commands over a longer time window.

7. A method as in claim 6, wherein the longer time window is longer than the time window in case of no gating by an amount such that the same number of power change commands are evaluated as in case of no gating.

8. A method as in claim 1, wherein the procedure uses one or more parameter values including a number N313 of consecutive out-of-sync indications, and/or a number N315 of successive in-sync indications, and/or a number T313 indicating a length of time, and/or a first threshold Q_{out} for minimum quality and/or a second threshold Q_{in} for minimum quality, and wherein the radio link to the radio access network is declared failed according to the procedure if N313 consecutive out-of-sync indications are determined and then a time interval of T313 units of time expires before N315 consecutive in-sync indications are determined, wherein an out-of-sync indication is determined whenever a quality metric for the downlink channel falls below the first threshold Q_{out} for minimum quality, and an in-sync indication is determined whenever the quality metric exceeds the second threshold Q_{in} for minimum quality.

9. A method as in claim 1, wherein the on periods and the off periods each correspond respectively to an on period and an off period of a duty cycle, and wherein at least one of the parameter values is changed from a broadcast or predetermined value by an amount that is based on the off period compared to a whole period of the on/off duty cycle.

10. A computer program product comprising a computer readable storage structure embodying computer program code thereon for execution by a computer processor, wherein said computer program

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 816

code comprises instructions for performing a method according to any of claims 1-9.

11. An application specific integrated circuit provided so as to operate according to a method as in any of claims 1-9.

12. An apparatus for use by a user equipment wireless communication terminal, comprising:

means for determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

means for varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure.

13. An apparatus as in claim 12, wherein the gated transmission corresponds to a gating of transmission power or a gating of only the power control commands or a gating of reception of the power control commands by the UE.

14. An apparatus as in claim 12, wherein the means for varying a procedure is configured to vary the procedure by changing how to measure a parameter value used by the procedure.

15. An apparatus for use by a user equipment wireless communication terminal, comprising:

a first component of a physical layer implementation of a protocol stack of a wireless terminal, for determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 817

a second component of a physical layer implementation, for varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure.

16. An apparatus as in claim 15, wherein the gated transmission corresponds to a gating of transmission power or a gating of only the power control commands or a gating of reception of the power control commands by the UE.

17. An apparatus as in claim 15, wherein the second component is configured to vary the procedure by changing how to measure a parameter value used by the procedure.

18. An apparatus as in claim 17, wherein the change in the procedure is to count occurrences of events corresponding to the parameter value only if the events occur during one or another of the on periods of the gated transmission, instead of counting occurrences of such events regardless of when the events occur.

19. An apparatus as in claim 17, wherein the change in the procedure is to count occurrences of events corresponding to the parameter for a period of time longer than in case of no gating.

20. An apparatus as in claim 19, wherein the procedure used to measure when the parameter value is changed includes evaluating power change commands received during a time window, and wherein the change in the procedure is to evaluate power change commands over a longer time window.

21. An apparatus as in claim 20, wherein the longer time window is longer than the time window in case of no gating by an amount such that the same number of power change commands are evaluated as in case of no gating.

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 818

22. An apparatus as in claim 15, wherein the procedure uses one or more parameter values including a number N313 of consecutive out-of-sync indications, and/or a number N315 of successive in-sync indications, and/or a number T313 indicating a length of time, and/or a first threshold Q_{out} for minimum quality and/or a second threshold Q_{in} for minimum quality, and wherein the radio link to the radio access network is declared failed according to the procedure if N313 consecutive out-of-sync indications are determined and then a time interval of T313 units of time expires before N315 consecutive in-sync indications are determined, wherein an out-of-sync indication is determined whenever a quality metric for the downlink channel falls below the first threshold Q_{out} for minimum quality, and an in-sync indication is determined whenever the quality metric exceeds the second threshold Q_{in} for minimum quality.

23. An apparatus as in claim 15, wherein the on periods and the off periods each correspond respectively to an on period and an off period of a duty cycle, and wherein at least one of the parameter values is changed from a broadcast or predetermined value by an amount that is based on the off period compared to a whole period of the on/off duty cycle.

24. A user equipment wireless communication terminal, comprising:

an apparatus as in claim 12; and

a transceiver for communicatively coupling with the radio access network, and configured to transmit to the radio access network.

25. A user equipment wireless communication terminal, comprising:

a radio front end;

BNSDOCID: <WO_____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 819

a processor communicably coupled to the radio front end; and

a memory coupled to the processor for storing a set of instructions, executable by the processor, wherein the instructions comprise:

determining on periods and off periods of a gated transmission in connection with receiving power control commands over a downlink channel of a radio access network; and

varying a procedure used to determine when to declare a radio link failure based on the gated transmission by actually and/or effectively varying a quality measurement period used in the procedure or a parameter value used in the procedure.

26. A system comprising a user equipment wireless communication terminal as in claim 24 or claim 25 and a radio access network including a wireless terminal for communicably coupling to the user equipment wireless terminal by transmitting downlink signals to the user equipment wireless communication terminal and by receiving uplink signals from the user equipment wireless communication terminal.

27. A system as in claim 26, wherein the wireless terminal of the radio access network is configured to:

determine that the uplink signals are being transmitted according to a gated transmission; and

gate the downlink signals to correspond to the uplink gating.

BNSDOCID: <WO____2007129180A2_I_>

IPR2025-01572
Apple EX1002 Page 820

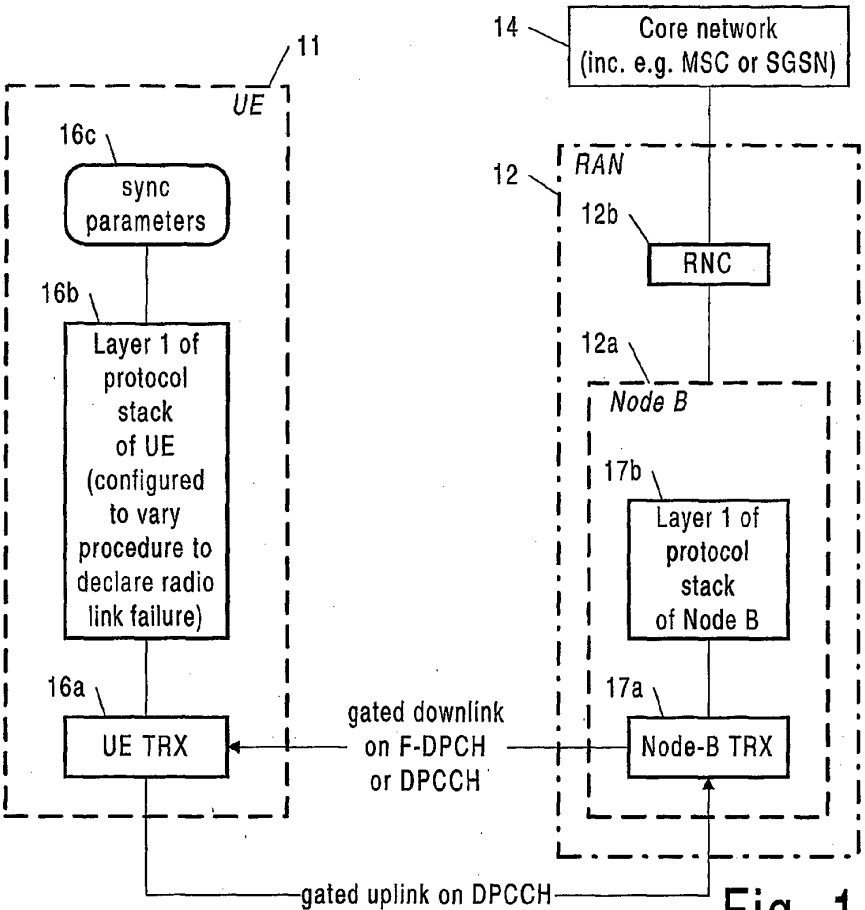


Fig. 1A

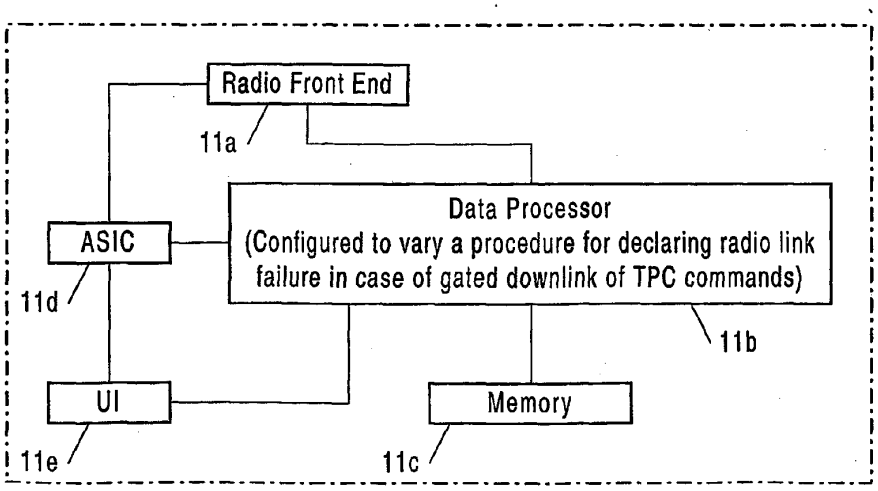


Fig. 1B

BNSDOCID: <WO_____2007129180A2_I_>

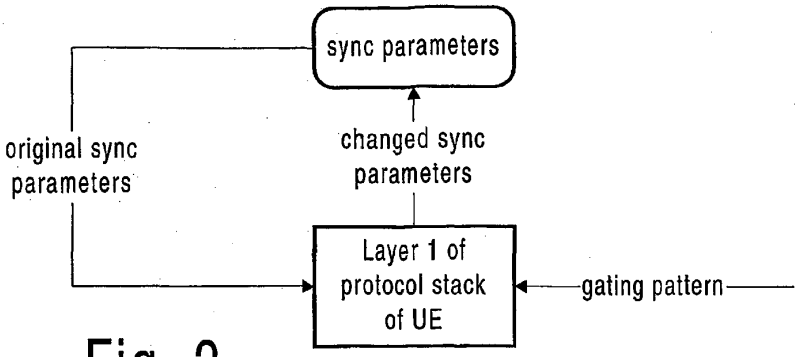


Fig. 2

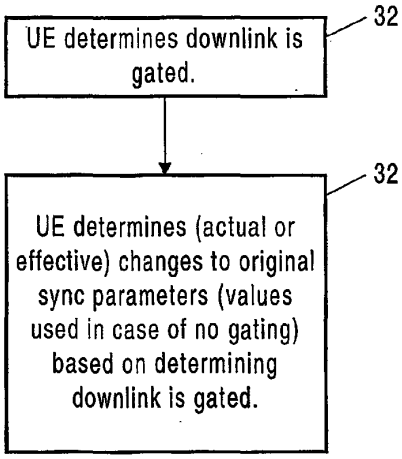


Fig. 3

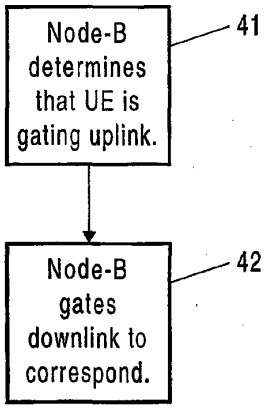


Fig. 4

BNSDOCID: <WO_____2007129180A2_I_>

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2007 (15.11.2007)

PCT

(10) International Publication Number
WO 2007/129180 A3

(51) International Patent Classification:
H04B 7/005 (2006.01) *H04Q 7/32* (2006.01)

(21) International Application Number:
PCT/IB2007/001120

(22) International Filing Date: 30 April 2007 (30.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/797,943 5 May 2006 (05.05.2006) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, Texas 75039 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KAIKKONEN, Jorma** [FI/FI]; Taskilantie 27 D 15, FIN-90580 Oulu (FI). **VIMPARI, Anna-Mari** [FI/FI]; Kummelintie 9, FIN-90520 Oulu (FI). **HINTZ-MADSEN, Mads** [DK/FI]; Luokkikuja 6, FIN-90310 Oulu (FI).

(74) Agents: **MAGUIRE, Francis, J.** et al.; Ware, Fressola, Van Der Sluys & Adolphson LLP, 755 Main Street, P.O. Box 224, Monroe, Connecticut 06468 (US).

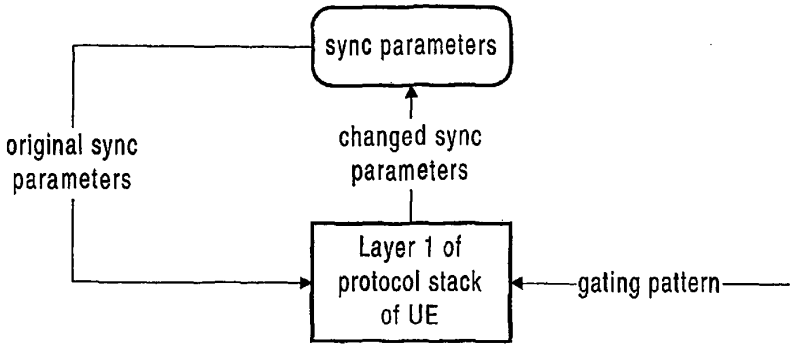
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, 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.

(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).

Published:
— *with international search report*

(88) Date of publication of the international search report:
28 February 2008

(54) Title: ENHANCED UE OUT-OF-SYNC BEHAVIOR WITH GATED UPLINK DPCCH OR GATED DOWNLINK F-DPCH OR DPCCH TRANSMISSION



(57) Abstract: A method and corresponding equipment by which a wireless terminal communicatively coupled to a radio access network adapts to gating in respect to a downlink signal from a radio access network carrying power control commands (e.g. the F-DPCH of UTRAN with WCDMA), including gating by the radio access network of either just the power control commands or the channel itself, or gating of reception of the power control commands by the user equipment. The adaptation can include changing values of parameters used in determining when the wireless terminal declares a radio link failure, or instead only changing the procedures used to determine whether a parameter value has been achieved and thus only effectively changing the parameter values (or one or more of the parameters can be actually and effectively changed).

WO 2007/129180 A3

BNSDOCID: <WO_____2007129180A3_I_>

IPR2025-01572
Apple EX1002 Page 823

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2007/001120

A. CLASSIFICATION OF SUBJECT MATTER

IPC: 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)

IPC: H04B, H04L, H04Q

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	3GPP TS 25.331 V6.9.0 (2006-03), paragraph 8.5.4, 8.5.6 --	1-27
A	3GPP TS 25.101 V6.11.0 (2006-03), 3rd Generation Partnership Project: Technical Specification Group Radio Access Network: User Equipment(UE) radio transmission and reception (FDD) (Release 6), paragraph 6.4.4 --	1-27
A	3GPP TS 25.214 V6.8.0 (2006-03), 3rd Generation Partnership Project: Technical Specification Radio Access Network: Physical layer procedures (FDD) (Release 6), page 9-page 13 --	1-27

[X] Further documents are listed in the continuation of Box C. [X] 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
6 December 2007	10 -12- 2007
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Anders Ackeberg/ABW Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (April 2007)

BNSDOCID: <WO_____2007129180A3_I_>

IPR2025-01572
Apple EX1002 Page 824

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2007/001120

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1083678 A1 (LUCENT TECHNOLOGIES INC.), 14 March 2001 (14.03.2001), paragraphs [0013]-[0016]	1-27
A	US 20020112288 A1 (LUNDBY, S ET AL), 15 August 2002 (15.08.2002), paragraphs [0025]-[0028],[0035]-[0037],[0045], figures 3B-C, claims 1-9, abstract	1-27
A	US 6493541 B1 (GUNNARSSON, F ET AL), 10 December 2002 (10.12.2002), column 5, figure 8, abstract	1-27
A	US 20050281222 A1 (RANTA-AHO, K ET AL), 22 December 2005 (22.12.2005), paragraph [0017], abstract	1-27
A	3GPP TSG RAN2#47 Athens, Greece, 9-13 May, 2005. Change Request: "Faster L1 DCH synchronization". Paragraph 8.5.6	1-27

Form PCT/ISA/210 (continuation of second sheet) (April 2007)

BNSDOCID: <WO____2007129180A3_I_>

International patent classification (IPC)
H04B 7/005 (2006.01)
H04Q 7/32 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **YGPZDTUMYO**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

BNSDOCID: <WO____2007129180A3_I_>

IPR2025-01572
Apple EX1002 Page 826

EP	1083678	A1	14/03/2001	CA	2316722	A	07/03/2001
				JP	2001103004	A	13/04/2001
				KR	20010050378	A	15/06/2001
				US	6571104	B	27/05/2003
US	20020112288	A1	15/08/2002	DE	10108635	A	19/09/2002
				JP	2002282238	A	02/10/2002
				US	6668403	B	30/12/2003
US	6493541	B1	10/12/2002	AU	6037800	A	22/01/2001
				TW	469708	B	21/12/2001
				WO	0103329	A	11/01/2001
US	20050281222	A1	22/12/2005	CA	2571423	A	05/01/2006
				EP	1759555	A	07/03/2007
				KR	20070030280	A	15/03/2007
				MX	PA06015030	A	08/02/2007
				WO	2006000876	A	05/01/2006

BNSDOCID: <WO_____2007129180A3_I_>

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 026 514 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.02.2009 Bulletin 2009/08

(51) Int Cl.:
H04L 12/56 (2006.01)

(21) Application number: **07425527.4**

(22) Date of filing: **14.08.2007**

(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 MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicants:
- **Nokia Siemens Networks S.p.A.**
  20126 Milano (IT)
- **Nokia Siemens Networks Oy**
  02610 Espoo (FI)

(72) Inventors:
- **Cavalli, Simona**
  21027 Ispra (VA) (IT)
- **Meago, Francesco**
  23100 Sondrio (IT)

(54) **Resource management method for multi acces networks**

(57) Every controller (RNC, BSC, E-NodeB, BS) of multi-RAT PLMN (UTRAN, GERAN, LTE, WiMAX) calculates for each controlled cell a MUB IE describing the availability of transport services in terms of maximum user bitrate that can currently be allowed to each transport service, separately for UL and DL, needed to plan usage of radio resources in the current and neighbouring cells, such as for handovers, cell reselections and new service setups. The MUB computation avails of:
-calculating an available capacity for a given service by taking a normalised capacity accessible to said service and by subtracting to it a normalized load of said service and of any other service that cannot be pre-empted by said service;
-calculating the MUBN for said service as the minimum between said available capacity and the maximum capacity MAXUB allowed to the single user for said service as a configuration setting;
-calculating a quantized representation MUB of the MUBN for said service as the nearest power of two raised at an integer n.

The MUB is included into management messages forwarded to the other controllers, either of the same or different technologies. Every controller checks the received MUB coming from the other controllers in order to decide on the most suited target cell, among the current and neighbouring cells, for resource management issues such as handover, cell reselection, and new service setup (fig.6).

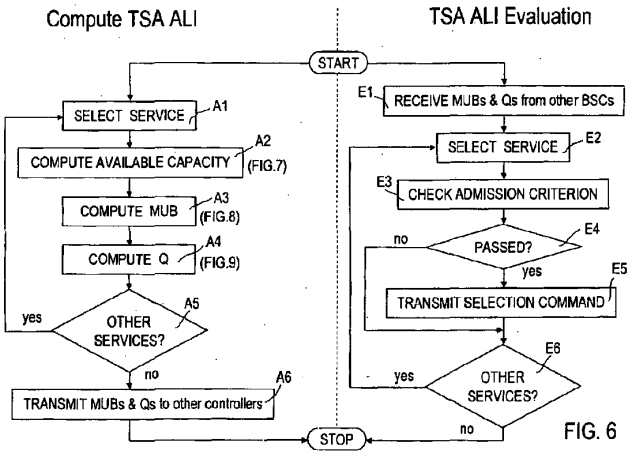


FIG. 6

Printed by Jouve, 75001 PARIS (FR)

EP 2 026 514 A1

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 828

Description

FIELD OF THE INVENTION

[0001] The present invention relates to the so-called Ambient Networks (AN), and in particular to a resource management method for multi-access networks. (Used acronyms description and bibliographic references are given at the end of the description).

BACKGROUND ART

[0002] The communications industry has a truly historic opportunity over the coming years to connect the majority of the world using mobile, wireless broadband and fixed broadband systems. As a result, in 2015 we will live in a world, in which five billion people are connected, most of them 'always on' with a broadband connection. People can use the services they want anytime, anywhere with their preferred devices.

[0003] The Internet will be the dominant platform to connect these five billion people and their various devices with each other, and to provide access to a great variety of content and applications. Mobility will dominate in voice services with 70-90% of all traffic, depending on the market.

[0004] Broadband IP connections will be available practically anywhere in the world, across developed and growth markets. A combination of mobile, wireless and fixed systems will ensure global coverage, full mobility and adequate speed and capacity. In the growth markets mobile and wireless broadband will play a crucial role in broadband coverage.

[0005] In the converged telecom, Internet, media and IT landscape there will be a much larger variety of services providers and business models compared to today's telecom environment. Each provider will compete in a larger market than traditionally seen, creating both a huge opportunity and increased competition.

[0006] Taking into account said converged landscape, future internetworking will continue to signify "the interaction of heterogeneous networks", today including cellular, wireless and wire-line networks, public and private, belonging to users and operators. In this context the Ambient Networks project (see Ref. [1], [2], and [3] at the end) works for specifying a system capable to handle future internetworking by enabling dynamic composition of networks and establishment of inter-network agreements, coexistence of multiple access technologies, multi-operator and multi-hop functions, mobility and security support. The vision for multi-access operations is characterized by heterogeneous access technologies, radio or fixed, through which data may flow in series (multi-hop) or in parallel, alternatively or concurrently.

[0007] To enable multi-access operations, efficient resource management methods need to consider the diverse characteristics of the heterogeneous access technologies. This translates into the need to identify how the dissimilar access resources should be abstracted in order to provide the most suited building block for resource management operations, optimizing the trade-off between performance of the adopted resource management schemes, and cost of signalling and processing as contextualized in today's technologies. Started in January 2004 as part of the IST 6th Framework Programme of the European Union, the Ambient Networks project is developing a new networking environment providing thorough inter-working among today's networks, characterized by their diverse features and services. The objectives include enabling the emergence of new businesses, as well as stimulating continuous growth in the communication market.

[0008] Ambient Networks described in Ref.[3] realizes its objectives through the definition of a new network convergence layer, the "Ambient Control Space" (ACS), as a control stratum typically referred to as an overlay, where the envisaged Ambient Networks functionality is introduced. Open implementation options exist how this networking realm should be realized, while the main interfaces are under specification process.

[0009] **Fig.1** schematizes a typical Ambient Network (AN) scenario characterised by the ACS as a control plane, and an Ambient Connectivity (ACY) functionality. The ACS includes a number of functionalities capable of managing Multi-radio Access, Context information, mobility, security and even more. The ACS includes interfaces towards the higher layers of control functionality, such as user applications through the Ambient Service Interface (ASI), and also includes Ambient Resource Interfaces (ARI) towards the ACY, i.e. the lower layers of control functionality. ANs and their respective ACSs interact through the ANI. ASI, ARI and ANI are logical interfaces that may run over heterogeneous communication means and access technologies.

[0010] The issue of multi-access in the ACS described in Ref.[4] mainly refers to criteria how resource management may handle communication paths of diverse access technology both in series and in parallel, alternatively or concurrently. For solving this issue, it is of primary importance to identify suitable abstractions of the access resource through which the ACS can view and control the "Ambient Connectivity" layers, where technology-specific communication paths are accessible via the "Ambient Resource Interface" (ARI). **Fig.2** schematizes a process involving both ACS and Ambient connectivity in which technology-specific information needs to be abstracted up to a level and to a type that allows provisioning the envisaged multi-access operations in the ACS through respective algorithms. To this aim, "Abstracted (load) information" is defined as a more generic type of information, typically technology-independent, or quasi-technol-

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 829

ogy-independent, obtained by transformation through algorithms (abstraction layer algorithms) from a technology specific information. The goal is therefore not only defining the most suitable abstractions, but also providing the related mechanisms and algorithms for the technology-specific Abstraction Layers, together with the related access selection and admission control algorithms for the ACS.

[0011] Cell Capacity/load abstractions have been suggested up to now within discussions around load balancing in 3GPP for achieving a timely specification enabling some coordination between RNCs and BSCs. Cell load is a measurement typically easy to retrieve from parameters like total transmitted power, interference, number of occupied timeslots, etc.

[0012] "Transport Service Availability" (TSA) abstraction, limitedly to the bearer service, is disclosed in Patent application EP-A1-1503606 of the same inventors, which describes: a common radio resource management method in a mobile radio communication network employing different radio access technologies that overlap over a geographic area subdivided into cells belonging to the domains of respective controllers which are connected to each other in overlapping or adjacent domains and to a core network by means of relevant interfaces, suitable to be carried out for each controlled cell by the respective controller through the steps of:

- starting from acquired information about QoS and throughput of all the active connections with the served mobile terminals (UE/MS), calculating traffic-related Information Elements, separately for uplink and downlink, needed to plan handovers and/or cell reselections; said traffic-related Information Elements including indications of the availability of bearer services in the cell in terms of maximum bitrate, either guaranteed or not guaranteed, that can currently be allowed to each bearer service, said bearer service being distinguished by traffic class due to the different QoS characteristics of the bearer services in terms of Eb/No, error rates, priorities, and delay;
- including said traffic-related Information Elements in management messages forwarded to the controllers of different cells to the one in turn considered, either of the same or different technologies;
- checking said traffic-related Information Elements coming from the other controllers (BSC, RNC) in order to decide either of issuing or preventing handovers and/or cell reselection commands towards a neighbouring cell.

OUTLINED TECHNICAL PROBLEM

[0013] The teaching of the aforementioned document EP-A1-1503606 was only directed to announce the Bearer Service Availability as an exemplary abstraction based on Transport Service, but none other than reference to generic tables it is said of how calculating the Bearer Service Availability, so it is not currently known how to produce Transport Service Availability information elements. Without an effective criterion of how calculating said TSA, the access network controllers originating the information cannot "forecast" the outcome of the resident admission control algorithms for the specific service to be admitted.

OBJECT AND SUMMARY OF THE INVENTION

[0014] The main object of the present invention is that to overcome the lack of a clear teaching in the prior art of how calculating a transport service availability information element.

[0015] The invention achieves said object by providing a radio resource management method in a mobile radio communication network employing different radio access technologies, e.g.: UTRAN, GERAN, LTE, WiMAX, that overlap over a geographic area subdivided into cells belonging to the domains of respective controllers (RNC, BSC, E-NodeB, BS), including the following steps carried out by every controller for each controlled cell:

a) calculating a transport service availability information element, called hereafter MUB, describing the availability of transport services in terms of maximum user bitrate that can currently be allowed to each transport service, separately for uplink and downlink, needed to plan usage of radio resources in the current and neighbouring cells, such as for handovers, cell reselections and new service setups; the computation at step a) including at least the following substeps executed for each implemented service characterised by service type and high/low priority:

a1) calculating an available capacity for a given service by taking a normalised capacity accessible to said service and by subtracting to it a normalized load of said service and of any other service that cannot be preempted by said service;

a2) calculating the MUBN for said service as the minimum between said available capacity and the maximum capacity MAXUB allowed to the single user for said service as a configuration setting;

a3) calculating a quantized representation MUB of the MUBN for said service for transmission over digital transmission means;

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 830

b) including said MUB information elements calculated as above into management messages forwarded to the other controllers, either of the same or different technologies;
c) checking said MUB information elements coming from the other controllers (BSC, RNC, E-NodeB, BS) in order to decide on the most suited target cell, among the current and neighbouring cells, for resource management issues such as handover, cell reselection, and new service setup, as described in claim 1.

[0016] Details on the calculation and other aspects of the invention are described in the dependent claims.

[0017] A radio resource management method which avails of the precise teaching of how calculating TSA information according to the present invention, constitutes an effective improvement of the access selection and admission control algorithms in the control space of the Ambient Networks.

[0018] The smartness of the method has been tested by means of a comparative emulation applied to a GSM access network between TSA Abstraction Layer Information (ALI) calculated according to the method of the invention and 3GPP ALI based on Cell capacity/load. To the only aim of the emulation, some algorithms have been appositely developed also for calculating 3GPP (GSM) ALI and successively using it in evaluating some selection criteria of target cells for a given service.

[0019] Finally, a comparative algorithm between performances of two types of ALI has been developed for calculating the admission control error probability versus minimum cell load using 3GPP ALI instead of TSA ALI in emulating a GSM scenario characterized by a single target cell. The outcome of the comparative algorithm is the bunch of error curves reported in **fig.10** which clearly attests the superiority of TSA ALI calculated according to the method of the invention: typically, gains are higher for higher cell load, i.e. in the most critical situations.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] The invention and its advantages may be understood with reference to the following detailed description of an embodiment thereof taken in conjunction with the accompanying drawings given for purely non-limiting explanatory purposes and wherein:

- **fig.1** shows an Ambient Control Space and Connectivity diagram of the so-called Ambient Networks;
- **fig.2** schematized the mechanisms involved with the abstraction paradigm used at the ARI interface between ACS and Connectivity of fig.1;
- **fig.3** shows a known diagram of a Multi-RAT (GSM + 3G) PLMN as an exemplary scenario of Ambient Network;
- **fig.4** shows a very general diagram of the exchange of TSA Abstracted Load Information (ALI) calculated according to the method of the present invention, between a GSM controller and another Access Controller which performs TSA-based evaluation algorithms for traffic planning inside the network of fig.3;
- **fig.5** shows a very general diagram which differs from the previous one for the additional exchange of traditional 3GPP ALI based on capacity /load, so at the other Access Controller two evaluation algorithms for access selection can be compared to each other in order to calculate the evaluation error of the 3GPP ALI approach in respect of more correct evaluations performed by the algorithm which makes use of TSA ALI calculated according to the method of the invention;
- **fig.6** is the most general flow chart of GSM abstraction layer for computation of TSA ALI and concurrent execution of TSA ALI evaluation for admission control according to the method of the invention;
- **figures 7, 8, and 9** are flow charts relevant to corresponding steps of the flow chart of fig.6;
- **fig.10** shows a bunch of 3GPP ALI error curves versus minimum cell load (plotted for various services) in taking cell selection decisions comparatively based on both 3GPP ALI and TSA ALI, when the GSM scenario of fig.5 is emulated limitedly to a single target cell;
- **fig.11** shows an evolution of the Multi-RAT PLMN depicted in fig.3 as a future candidate to host the present invention;
- **fig.12** shows a diagram of inter E-Node B communication according to 3GPP Long Term Evolution (LTE) Access Network as another candidate to host the present invention;
- **fig.13** shows a similar diagram for a WiMAX Access Network as still another candidate to host the present invention.

DETAILED DESCRIPTION OF AN EMBODIMENT OF THE INVENTION

[0021] **Fig.3** shows a multi-RAT (Radio Access Technology) PLMN that will be soon completed in Europe. The new Universal Mobile Telecommunications System (UMTS) shares the existing GSM (Global System for Mobile communications) Core Network CN with the GPRS service. Relevant GSM RAN (Radio Access Network) in fig.3 is the so-called GERAN (GSM EDGE RAN), corresponding to the ultimate GSM RAN based on new EDGE (Enhanced Data rates for GSM Evolution) techniques that allow higher data rates in GSM, e.g. higher modulations. The Core Network CN is connected to one or more BSS (Base Station Subsystem) of the GSM, and to one or more RNS (Radio Network

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 831

Subsystem) of an UTRAN (Universal Terrestrial Radio Access Network). The UMTS system of fig.3 is described in the TS 23.002 (CN) and TS 25.401 (UTRAN). Both the UTRAN and BSS are connected, on air, to a plurality of User Equipment UE/MS, each including a Mobile Equipment ME with a respective USIM card (UMTS Subscriber Identity Module). The present invention applies to UEs of single but preferably multistandard type: so that they are indicated as UE/MS (without limitation, often the only term UE is indicated). The UTRAN includes a plurality of Node B blocks each connected to a respective Radio Network Controller RNC by means of an Iub interface. A node B includes a Base Transceiver Station BTS connected to the UEs through an on-air Uu interface. The upper RNC is a Serving S-RNC connected to the Core Network CN by means of a first Iu(CS) interface for Circuits Switched and a second Iu(PS) interface for Packet Switched of the GPRS. It is also connected to an Operation and Maintenance Centre (OMC). The RNC placed below can be a Drift D-RNC and is connected to the upper S-RNC by means of an Iur interface. The UTRAN with the served UEs constitute a Radio Network Subsystem (RNS) disclosed in TS 23.110.

[0022] The GSM - BSS block includes a plurality of BTSs connected to a Base Station Controller BSC by means of an Abis Interface and to the UEs through an on-air Um interface. The BSC is interfaced to the Core Network CN by means of a Gb interface (packet switched) and is further connected to a Transcoder and Rate Adaptor Unit TRAU also connected to the Core Network CN through an A interface. It is also connected to an Operation and Maintenance Centre (OMC).

[0023] The CN network includes the following Network Elements: Switching Centre MSC / Visitor Location Register VLR, Gateway MSC GMSC, Interworking Function IWF / Transcoder TC, Camel Service Environment CSE, Equipment Identity Register EIR, Home Location Register HLR, Authentication Centre AuC, Serving GPRS Support Node SGSN, and Gateway GPRS Support Node GGSN. The following interfaces are visible inside the CN block: A, E, Gs, F, C, D, Gf, Gr, Gc, Gn, and Gi. The IWF block translates the Iu(CS) interface into the A interface towards MSC / VLR block. The TC element performs the transcoding function for speech compression/expansion concerning UTRAN (differently from GSM where this function is performed outside the CN network) also connected to the MSC block through the A interface. The GMSC is connected to the MSC / VLR through the E interface and to a Public Switched Telephone Network PSTN and an Integrated Services Digital Network ISDN. Blocks CSE, EIR, HLR, AUC are connected to the MSC / VLR through, in order, the Gs, F, C, and D interfaces, and to the SGSN node through the Gf and Gr interfaces. The SGSN block is interfaced at one side to the S-RNC inside UTRAN block by means of the Iu(PS) interface, and to the BSC inside the GSM-BSS block through the Gb interface. At the other side the SGSN node is interfaced to the GGSN node through the Gn interface. The last block is connected through the Gi interface to a packet data switching network of the IP (Internet Protocol) type and/or the X.25 type. The Core Network CN of fig.3 consists of an enhanced GSM Phase 2+, as described in TS 23.101, with a Circuit Switched CS part and a packet Switched part (GPRS). Another important Phase 2+ is the CAMEL (Customised Application for Mobile network Enhanced Logic) Application Part (CAP) used between the MSC and CSE for Intelligent Network (IN) applications. CAP is described in TS 29.078.

[0024] In operation, the MSC, so as the SGSN node, keep records of the individual locations of the mobiles and performs the safety and access control functions. More BSS and RNS blocks are connected to the CN Network, which is able to perform intrasystem handovers between adjacent RNSs or between adjacent BSSs, and intersystem handovers between a RNS and an adjacent BSS. UTRAN in respect of GSM further improves data service by making possible greater throughputs and the asymmetrical traffic typical of the Internet Protocol (IP). The network of fig.3, which only represents a minimal part of a world-wide network, shall allow the routing of a telephone call inside an International UMTS / GSM Service Area subdivided into National Service Areas. By way of the hierarchical structure of the network, each National Service Area is subdivided into the following nested domains of decreasing area: PLMN Service Area; MSC / SGSN Service Area; Location Area LA (CS-domain) uniquely defined by its LAI (Location Area Identity) code; Routing Area RA inside the SGSN Service Area as a partition of the CS Location Area; Cell Area where the UE is actually located in the radio coverage of a target Node B or BTS. Many known protocols described in the relevant standardization are deputed to govern the exchange of information at the various interfaces.

[0025] To the aim of the present invention the multi-RAT network of **fig.3** is a particular embodiment of the Ambient Network of **fig.1** whose controllers RNC and BSC are capable of handling TSA ALI calculated as will be described soon. More in particular, the functional blocks indicated in **figures 4** and **5** are mapped in the network of **fig.3.**

[0026] Referring also to **figures 11** to **13** for what concerns the SAE/LTE and WiMAX technologies, this figures being explained later in detail, we describe a method where different access technologies (including UTRAN, GERAN, LTE and WiMAX) totally or partially overlapping over a geographic area, or having respective neighbouring cells, are coordinated through their respective controllers (RNC, BSC, E-NodeB, BS, ...) for the sake of handovers, cell reselections and new service setups. The method is based on the calculation, exchange and evaluation of TSA information, including indication of the maximum user bitrate (MUB) and quantity (Q) that can currently be allowed to the single user for each service.

[0027] Now with reference to the **figures 6** to **9** a TSA ALI computation algorithm is described limitedly to the GSM case for the BSC, but this shouldn't constitute a bar for the skilled in the art in adapting the algorithm to the UTRAN or other RAT networks. Parallelly to the description of the TSA ALI computation algorithm a 3GPP ALI computation algorithm

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 832

is described to the only aim of comparison between the twos and without dedicated figures.

[0028] We consider for GSM a number of transport service types including conversational circuit-switched services, Enhanced GPRS streaming services, non-real-time GPRS services and non-real-time Enhanced GPRS services. Also, we consider different service priorities for a portion of the described service types: in particular we consider as higher priority services the ones in handover, and as lower priority services any new service setup request.

[0029] We start describing the algorithm for computing the TSA information described in **fig.6 (leftmost part).** For each service (**fig.6**, steps A1 and A5), characterised by service type and service priority, we compute the available capacity (step A2), then we compute the MUB (step A3) and finally we compute the additional element Q (step A4) describing the quantity of available services at the bitrate indicated by MUB.

[0030] For computing the available capacity for a given service, we start by computing the accessible capacity to that service, which equals at first the total fixed cell capacity. However, when taking into account reserved capacities for different services, the accessible capacity for that service needs to exclude any capacity reserved to other services, for example resources reserved to circuit switched and/or packet switched services (**fig.7** step C1). In particular, reserved resources can be dynamically set in time according to policies, current resource usage and resource bookings.

[0031] Moreover, the accessible capacity is either all capacity accessible to the given service type for the highest service priority of that service, or a percentage of all capacity accessible to the given service type according to a respective load threshold set for lower service priorities (**fig.7** steps C2 and C3). When taking into account reserved capacities for different services, load thresholds for lower service priorities can be set on the reserved and shared capacities limiting the accessible capacity for those service priorities accordingly to a related portion.

[0032] Having computed the accessible capacity, its current occupation in terms of load needs to be considered. When there exist non-guaranteed resources given as a surplus resource to any service, the guaranteed load of any service needs to be computed as the current load in the portion required for providing a guaranteed Quality of Service, excluding any surplus resource currently allocated (**fig.7** step C4).

[0033] The available capacity for a given service is then computed (**fig.7** step C5) by taking the capacity accessible to the service and by subtracting to it the guaranteed load of that service and of any other service that cannot be pre-empted by that service. When taking into account reserved capacities for different services, the load of any other service that cannot be pre-empted by that service would be considered only in the portion of allocation into the capacity accessible to that service. Finally, when taking into account additional control signalling load, the available capacity for a given service would need not to include the capacity allocated for control signalling in the portion of allocation into the capacity accessible to that service.

[0034] The available capacity, together with the accessible capacity and the load of different services, can be computed in a number of ways, for example as a bitrate indication or a pure number. When computing it as a bitrate indication a normalisation criteria is required: for example for any service the capacity available can be computed first as a gross normalised bitrate as if the capacity available would be used by a reference service (e.g. voice), and only in a second step the capacity available can be expressed as net user bitrate through a conversion factor (**fig.7** step C6).

[0035] Once computed the available capacity for a given service, taking into account the maximum capacity MAXUB allowed to the single user for that service as a configuration setting, the algorithm needs to compute MUBN as the minimum between the available capacity and MAXUB (**fig.8** step M1). In particular, MAXUB can be dynamically set in time as a function of the available capacity. The algorithm then computes for the given service the TSA parameter MUB as a quantized representation of MUBN, for the sake of transmission over digital transmission means (**fig.8** step M2). This can be done in a number of ways, e.g. by taking the integer part of MUBN, or by taking the nearest power of two raised at an integer n.

[0036] Once computed MUB, and in particular MUBN, the algorithm computes QN describing the number of available services of bitrate MUBN as the ratio between the available capacity and MUBN (**fig.9** step Q1). Finally the algorithm computes for the given service the TSA parameter Q as a quantized representation of QN, for the sake of transmission over digital transmission means (**fig.9** step Q2). This can be done e.g. through thresholds on QN distinguishing a number of quantity levels.

[0037] When TSA is computed for each service of interest in terms of MUB and Q, this information is passed to other access controllers (**fig.6** step A6), which on need will use this information for performing access selection for a given service (**fig.6** step E1).

[0038] With regards to the access selection algorithms, **fig.6 (rightmost part)** describes the undertaken steps. First of all, a service is selected (**fig.6** step E2) for which an access selection decision needs to be taken, based e.g. on handover/cell reselection needs, new service requests and load management needs.

[0039] Regarding the access selection criterion (**fig.6** step E3) there exist two cases: the case where a single cell is evaluated as a potential target, and the case where two or more cells are compared as potential targets. In both cases the algorithms need to take the TSA information corresponding to that service. In the former case the algorithm needs then to check if the MUB information indicates the availability of the required bitrate for that service, in which case the cell is a suitable target cell. In the latter case instead the algorithm needs then to check if the MUB information indicates

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 833

the availability of the required bitrate for that service in each cell, in which case the cells satisfying this requirement are suitable target cells, and if required finally check the Q information element of the different suitable target cells for selecting the cell with highest Q as the best target cell.

[0040] If a target cell could be selected (**fig.6** step E4), a selection command is transmitted (**fig.6** step E5), triggering e.g. handover/cell reselection requests of service setup requests towards the target cell. Concluding, the algorithm may be repeated for any additional service requiring access selection (**fig.6** step E6).

General assumptions

[0041]

- UUDL: in general, similar parameters and characteristics apply for uplink and downlink. For simplicity we refer e.g. to only DL for calculation and evaluation of the TSA, although similar work should be done for UL. Also, an aggregated figure could be obtained for UL and DL by combining the TSA for UL and DL.
- there exist resources reserved for different services (voice, GPRS) and priorities (voice handover), and/or vendor specific thresholds (e.g. new calls will be accepted only under 75% load). We assume for simplicity that for each service dedicated (reserved) resources are filled first, i.e. that the system can be configured as such.
- there exists a varying capacity occupied by signalling and other overheads (broadcast channels, coding, signalling for call setup, ...)
- there exist surplus resources, i.e. resources that are given to the user as a surplus, i.e. above the guaranteed bitrate, under favourable conditions. This exists only for RT services, as for NRT nothing is guaranteed. E.g. it considers the allocation of full-rate codecs or high-quality AMR codecs, that can be given under favourable load conditions, but which availability cannot be guaranteed.
- there exist different classes of terminals with different values for max throughput that can be provided to the user. Also, due to particular interference conditions, different terminals may adopt more or less favourable coding schemes. Still, we don't use these assumptions because the described realization of TSA is agnostic of the specific user exploiting the service.

DEFINITION OF ABSTRACTED RESOURCES

GSM Resource Status (RS)

[0042] The following characterization is defined in order to build the abstraction layers on something concrete. The information elements presented have the following requirements:

- They need to represent technology-specific resource abstractions.
- They need to significantly describe the status of the resources.
- They need to be obtainable, i.e. it must be possible to calculate them through specific modules.

[0043] We characterize GSM resource status (RS) as follows:

- C: a total fixed capacity, depending on the number of TRX/channels, in normalised kbit/s (normalised for a typical channel, e.g. voice under normal conditions - gross occupancy) [182.4 .. 8755.2 kbit/s]
- C(C), C(P): set of resources reserved to circuit (C) and packet (P) services [0 .. 8755.2 kbit/s]
- L: load parameter in normalised kbit/s indicating the gross total occupancy [0 .. 8755.2 kbit/s]
- L(RTC): load parameter in normalised kbit/s indicating the gross occupancy due to circuit RT services (voice) [0 .. 8755.2 kbit/s]
- L(RTP): load parameter in normalised kbit/s indicating the gross occupancy due to packet RT services (streaming)

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 834

[0 .. 8755.2 kbit/s]

- L(NRT): load parameter in normalised kbit/s indicating the gross occupancy due to (packet) NRT services [0 .. 8755.2 kbit/s]

- L(S): load parameter in normalised kbit/s indicating the gross occupancy due to overheads including call signalling, L2 overheads and other overheads (BCCH, ... overhead not yet included in other parameters L(RTC), L(RTP), L (NRT)). [0 .. 8755.2 kbit/s]

- K(service): parameter indicating for every service the ratio between the net kbit/s of the user service (maximum for the best case, while possible) and the gross normalised kbit/s of the same service [k(service)].

    o k(conv) = 13 / 22.8 = 0.570

    o k(str) = 59.2 / 22.8 = 2.596

    o k(GPRS NRT) = 21.4 / 22.8 = 0.939

    o k(EGPRS NRT) = 59.2 / 22.8 = 2.596

- O(RTC): load parameter in normalised kbit/s indicating within L(RTC) the gross occupancy due to SURPLUS RT circuit services [0 .. 8755.2 kbit/s]. O(RTC)<L(RTC)

- O(RTP): load parameter in normalised kbit/s indicating within L(RTP) the gross occupancy due to SURPLUS RT packet services [0 .. 8755.2 kbit/s]. O(RTP)<L(RTP)

- S: load threshold above which the system does not accept requests for new guaranteed services (e.g. 0.75 (75%)).

[0044] 3GPP ALI (it is only used for the comparison with TSA ALI)
From 3GPP specifications, abstracted load information is characterized as follows:

- UL CCC: cell capacity class [1..100]
- DL CCC: cell capacity class [1..100]
- UL LV: load value [0..100] (linear, percentage of capacity)
- DL LV: load value [0..100]
- UL RTLV: RT load value [0..100] (linear, RT percentage of load value)
- DL RTLV: RT load value [0..100]
- UL NRTLI: NRT load indication [0..3] (low, medium, high, overload)
- DL NRTLI: NRT load indication [0..3]

TSA ALI (GSM)

[0045] We characterize abstracted load information in terms of "Transport Service Availability" (TSA), defined as follows:

- UL/DL information may be communicated separately or jointly.
- conversational TSA
- EGPRS streaming TSA
- GPRS NRT TSA
- EGPRS NRT TSA
- TSA includes: 1 bit for priority (high = 1, any = 0); 5 bits for max user bitrate according to a table, 1 bit for a quantity indicator (few / many).

ABSTRACTION LAYER ALGORITHMS

[0046] Abstraction layer algorithms are given for both 3GPP ALI and TSA ALI.
[0047] These algorithms are candidate for inclusion in the GLL Abstraction Layer, or in the abstraction layers below the ACS in general.

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 835

Algorithms GSM RS → 3GPP ALI (it is only used for the comparison with TSA ALI) Assumption:
MPL = 0.95 (maximum planned load as a fraction of the maximum capacity).
Algorithms:
CCC = C / 182.4 (in this way CCC will go from 1 to 48, allowing other technologies to go further up)
LV = (L / (C x MPL)) x 100
L(RT) = L(RTC) + L(RTP)
RTLV = (L(RT) / L) x 100
NRTOCC = L(NRT) / (C - L(RT) - L(S))
NRTLI = 0 [NRTOCC < 0.3]; 1 [NRTOCC < 0.6]; 2 [NRTOCC < 0.9]; 3 [NRTOCC ≥0.9].
Algorithms GSM RS → TSA ALI (GSM) (is part of the invention)
Assumptions:
prio = priority
MAXUB(service, prio) = maximum capacity that the system can give to a single user as a configuration setting. It may be allowed to vary depending on load condition (e.g. the higher the load, the smaller MAXUB)
CATS(service, prio) = Considerable Amount of Transport Services: threshold on the number of transport services determining discrimination between availability in quantity "few" or "many" for the same transport service. E.g. CATS = 2.

Algorithms:

[0048] With reference to **fig. 6 (leftmost part)**, the TSA ALI computation algorithm starts with the execution of step A1 in which one out of n foreseen services is selected; in the successive step A2 the Available Capacity is calculated as will be illustrated in **fig.7.** The sequential steps A3 and A4 are devoted to computation of MUB (**fig.8**) and Q (**fig.9**) parameters: MUB is the maximum capacity that the system can give to a single user according to Cavail and configuration settings. MUB can be expressed as an integer: note that an integer value already represents a quantization of a real value. In real messaging, it would need to be coded in a more compact format, e.g. by using n, where 2 at the power of n would indicate the approximate maximum user bitrate. Quantity QN indicates the available number of described bearers or transport services, while Q is a quantized description of QN indicating e.g. whether few (0) or many (1) of the described bearers are available. In the next step A5 the computation is iterated to the other services. When all services are completed, the BSC transmits MUB and Q Information Elements (IE) to other controllers in step A6. Alternatively, the transmission might be executed inside the loop.

[0049] With reference to **fig.7**, for any service and prio the Available Capacity is calculated as indicated in steps C1 to C6 described hereafter for the various services:

```
*/for all services /*
GL(RTC) (Guaranteed L(RTC)) = L(RTC) - O(RTC)
GL(RTP) = L(RTP) - O(RTP)
GL(RT) = GL(RTC) + GL(RTP)
*/ conversational /*
if GL (RTP) < C(P)
Cavail(conv, any prio) = (C - C(P) - GL(RTC) - L(S)) x k(conv)
else Cavail(conv, any prio) = (C - GL(RT) - L(S)) x k(conv)
if GL(RT)/C > S ≥Cavail(conv, prio 0) = 0
*/ streaming /*
if GL(RTC) < C(C)
Cavail(str, any prio) = (C-C(C)-GL(RTP)-L(S)) x k(str)
else Cavail(str, any prio) = (C-GL(RT) - L(S)) x k(str)
if GL(RT)/C > S → Cavail(str, prio 0) = 0
*/ NRT /*
if GL(RTC) < C(C)
Cavail(NRT) = C-C(C) - GL(RTP)-L(NRT) - L(S)
else Cavail(NRT) = C-GL(RT) - L(NRT)-L(S)
Cavail(GPRS NRT, any prio) = Cavail(NRT) x k(GPRS NRT)
Cavail(EGPRS NRT, any prio) = Cavail(NRT) x k(EGPRS NRT).
    With reference to fig.8 and fig.9, for any service and prio,
if Cavail(service, prio) ≥MAXUB(service, prio) then {
MUBN(service, prio) = MUB(service, prio) = MAXUB(service, prio);
QN = Cavail(service, prio) / MAXUB(service, prio);
if QN > CATS(service, prio) then Q(service, prio) = 1 else Q(service, prio) = 0;}
else {
MUBN = Cavail(service, prio);
```


BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 836

```
MUB(service, prio) = int (MUBN);
QN(service, prio) = Q(service, prio) = 0;}
endif
```

ALI EVALUATION ALGORITHMS

[0050] Algorithms are given for both 3GPP ALI and TSA ALI.

[0051] These algorithms are candidate for inclusion in MRRM, or in access selection algorithms within the ACS in general.

3GPP ALI evaluation algorithm (it is only used for the comparison with TSA ALI). Input variables: service, 3GPP ALI info of candidate target cells

Note: the (100 - Cell_Load) x Cell_Capacity_Class gives the absolute free capacity in the cell. This is what needs to be compared in order to decide the best cell load-wise, in order to take into account different cell sizes.

Note: thresholds mechanisms are not included because we assume LV is relative to "the maximum planned load".

[0052] We do not make straight connection between CCC and kbit/s because it was not meant by the 3GPP solution to do so.

service: conversational RT, streaming RT, GPRS NRT, EGPRS NRT;

```
if there is only one candidate target cell
ranking = 0 (i.e. service cannot fit in)
if (service = RT and LV < 100) ranking = 1 (i.e. service can fit in)
if (service = NRT and NRTLI < 3) ranking = 1
if there are two candidate cells (1, 2) to be compared
ranking(1) = 0;
ranking(2) = 0;
freecapacity:
FC(1) = (100-LV(1)) x CCC(1);
FC(2) = (100-LV(2)) x CCC(2);
if (service = RT)
if FC(1) ≥FC(2) and FC(1) > 0 then
 ranking(1) = 1;
 else
 if FC(2) > 0 then ranking(2) = 1;
endif
endif
if (service = NRT)
if NRTLI(1) ≤NRTLI(2) and NRTLI(1) < 3 then
 ranking(1) = 1;
 else
 if NRTLI(2) < 3 then ranking(2) = 1;
endif
endif
```

TSA ALI evaluation algorithm (is part of the invention)

[0053] With reference to **fig. 6 (rightmost part)**, the TSA ALI Evaluation algorithm starts with the execution of step E1 in which MUBs and Qs IEs transmitted by other BSCs are received. The successive steps E2 to E6 is a loop to check for each service the access selection criterion and, if passed, transmit an access selection command for that service towards a target cell. In the following the TSA ALI Evaluation algorithm is better detailed. Input variables: service, prio, bitrate, TSA ALI info of candidate target cells

```
if there is only one candidate target cell
if MUB(service, prio) ≥bitrate then ranking = 1; else ranking = 0;
if there are two candidate cells (1, 2) to be compared:
ranking(1) = 0;
ranking(2) = 0;
if Quantity(1, service, prio) ≥Quantity(2, service, prio) and MUB(1, service, prio) ≥bitrate
then
ranking(1) = 1;
else
if MUB(2, service, prio) ≥bitrate then ranking(2) = 1;
```


BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 837

```
endif.
```

EVALUATING TSA vs. 3GPP ALI PERFORMANCES (calculates the curves of **fig.10**)

[0054] Now 3GPP and TSA approaches are compared within a scenario characterized by a single target cell, where a controller has to decide if a given service fits or not in the target cell based on the ALI.

[0055] The comparative evaluation algorithm provides estimation of the difference in admission control success rate implied by use of 3GPP ALI vs. TSA ALI. By performing the evaluation for different values of minimum cell load, we obtain curves. The method is rather fast, since each RS configuration is considered only once.

[0056] The comparative algorithm does not emulate variations in the RS that could allow measuring the effects of aged information on both 3GPP ALI and TSA ALI. However, results show that TSA performs better then capacity/load even when generation and evaluation of the abstractions are done simultaneously.

[0057] Variables and parameters considered in the evaluation includes: Service type; Resource status.

Service type

[0058] The following service types are considered:

1. Conversational, MUB =13 kbit/s (Max User Bitrate), prio = 1 (e.g. handover)
2. Conversational, MUB =13 kbit/s, prio = 0 (e.g. new service request)
3. EGPRS streaming, MUB = 59.2 kbit/s, prio = 1
4. EGPRS streaming, MUB = 59.2 kbit/s, prio = 0
5. GPRS NRT, MUB = 21.4 kbit/s
6. EGPRS NRT, MUB = 59.2 kbit/s

Resource Status (RS)

[0059] The RS Information elements: C, C(C), C(P), L, L(RTC), L(RTP), L(NRT), L(S), K(channel), O(RTC), O(RTP) and S have been already defined.

Setting GSM RS parameters and variable limits

[0060] In the following, we assign values to GSM RS parameters and variable limits. Parameters:

- TRX = 182.4 kbit/s
- C = 5 x TRX kbit/s
- C(C) = 2 x TRX kbit/s
- C(P) = 1 x TRX kbit/s
- K(channel):
    - o k(conv) = 13 / 22.8 = 0.570
    - o k(EGPRS str) = 59.2 / 22.8 = 2.596
    - o k(GPRS NRT) = 21.4 / 22.8 = 0.939
    - o k(EGPRS NRT) = 59.2 / 22.8 = 2.596
- S = 0.75
- Sigmin = 0.04
- Sigmax = 0.08
- Op = 0.5
- Step = 8 kbit/s
- StepSig = 0.01
- Lmin: 60% = 0.6*C = 1094.4 kbit/s (we emulate loaded situations only, therefore the overall load ≥Lmin)

Variable limits:

- L [C x Lmin .. C kbit/s]
- L(RTC) [0 .. (C - C(P)) kbit/s]
- L(RTP) [0 .. (C - C(C)) kbit/s]

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 838

- L(NRT) [0 .. (C - C(C)) kbit/s]
- L(S) [Sigmin x L .. Sigmax x L kbit/s]
- O(RTC) [0 .. Op x L(RTC)]
- O(RTP) [0 .. Op x L(RTP)]

COMPARATIVE EVALUATION ALGORITHM

[0061] This algorithm goes through each configuration of interest for the RS and performs evaluation.

```
Count = 0;
Errcount(..) = 0;
Cc = C-C(P);
For L(RTC) = 0 to Cc step = Step
{ Coc = Op x L(RTC);
Cp = min (C-C(C), C-L(RTC));
For O(RTC) = 0 to Coc step = Step
{ For L(RTP) = 0 to Cp step = Step
  Cop=Op x L(RTP);
 { For O(RTP) = 0 to Cop step = Step
   { Lrt = L(RTC) + L(RTP);
     Cnrt= Cp - L(RTP);
     For L(NRT) = 0 to Cnrt step = Step
     { Lt = Lrt + L(NRT);
      For Sig = Sigmin to Sigmax step StepSig
      { L(S) = Lt x Sig;
        L = Lt + L(S);
        if L ≤C and Lmin < L
        { Count = Count + 1;
          For any service:
          { Errcount(service) = Errcount(service) + XOR (ALlevaluation(service,
3GPP ALI (RS)), ALlevaluation(service, TSA ALI (RS));}}}}}}}}.
```

[0062] The next **figures 11, 12,** and **13** report some future 3GPP and WiMAX network architectures candidate to host the present invention.

[0063] With reference to fig.**11**, 3GPP System Architecture Evolution (SAE) is a recent architectural development for the 3GPP system reported as a feasibility study in 3GPP TR 23.882 v1.9.0, "3GPP System Architecture Evolution: Report on Technical Options and Conclusions (Release 7)", March 2007.

[0064] SAE is composed by an Evolved Packet Core (EPC) that connects to several access networks, other core networks (including the legacy GPRS core network) and external elements. External elements include Policy and Charging Rules Function (PCRF, interface S7), Home Subscriber Server (HSS, interface S6), Operator IP Services or external Packed Data Networks (interface SGi). In particular, EPC connects to several access networks including Evolved RAN (also called LTE RAN, interface S1), trusted non-3GPP IP access including trusted fixed IP access (interface S2a), VVLAN access network. Within the EPC, the Mobility Management Entity (MME) and User Plane Entity (UPE) connect to the Evolved RAN (interface S1), the enhanced Packet Data Gateway (ePDG) connects to the VVLAV access network, while the inter Access System Anchor (IASA) connects to trusted non-3GPP IP access (interface S2a) and external Packet Data Networks (interface SGi). Regarding the elements within EPC, MME/UPE connects to IASA through interface S5a, IASA connects to ePDG through interface S2b. IASA is formed by the two additional elements 3GPP Anchor and SAE Anchor connected through S5b. EPC and GPRS Core networks may be interconnected in several ways (interfaces S3 and S4), for example through MME/UPE or through IASA. It should be noted that the presented SAE architecture is not the finalized architecture model for the evolved system, i.e. it does not contain all functions/interfaces required, and some functions/interfaces may be added, deleted or modified in the course of the key issue discussions within 3GPP.

[0065] With reference to fig.**12**, 3GPP Evolved RAN, or Long Term Evolution (LTE) RAN, or evolved UTRAN (E-UTRAN), is a recent architectural development for future 3GPP radio access networks, described in 3GPP TR25.813 v710. The LTE RAN is composed by Enhanced-NodeBs (E-NodeBs), directly interfacing to user terminals through antennas, connected to each other through interface X2, and connected to the EPC and in particular to an access Gateway through the interface S1 already described.

[0066] With reference to fig.**13**, the WiMAX Access Network is another access network being described in the IEEE 802.16 protocol suite and in documents originated by the WiMAX Forum. The WiMAX Access Network is composed by Base Stations (BS), directly interfacing to user terminals through antennas, possibly connected to each other through

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 839

respective interfaces, and connected to the Edge Router (also called Broadband Remote Access Server) through a respective interface. The WiMAX Access Network can connect to the 3GPP system via a Packet Data Gateway, ePDG or through an external Packet Data Network like the Internet.

[0067] In particular, TSA information along with its elements MUB and Q can be exchanged between entities such as E-NodeB, Access Gateway, MME/UPE, IASA, EPC, GPRS Core, BS, Edge Router and the controllers of any access network on the respective interfaces. For a GSM cell, TSA information can be exchanged between GERAN, GPRS Core and EPC, towards any relevant controller.

USED ACRONYMS

[0068]

3GPP	3rd Generation Partnership Program
ACS	Ambient Control Space
ALI	Abstracted Load Information
AMR	Adaptive Multi-Rate
AN	Ambient Network
ANI	Ambient Networks Interface
ARI	Ambient Resource Interface
ASI	Ambient Service Interface
BCCH	Broadcast Control CHannel
BS	Base Station
BSC	Base Station Controller
CS	Circuit Switched
DL	Downlink
E-NodeB	Enhanced NodeB
e-PDG	Packet Data Gateway
EGPRS	Enhanced GPRS
EPC	Evolved Packet Core
FC	Free Capacity
GERAN	GSM EDGE Radio Access Network
GLL	Generic Link Layer
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HP	High Priority
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IASA	Inter Access System Anchor
IE	information Element
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IST	Information Society Technologies
LP	Low Priority
LTE	3GPP Long Term Evolution
MME	Mobility Management Entity
MPL	Maximum Planned Load
MRRM	Multi-Radio Resource Management
NRT	Non Real Time
NRTLI	Non Real Time Load Information
NSN	Nokia Siemens Networks
NW	Network
PCRF	Policy and Charging Rules Function
PS	Packet Switched
PSS	Packet-Switched Streaming service
QoS	Quality of Service
RA	Routing Area
RAN	Radio Access Network

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 840

RAT	Radio Access Technology
RNC	Radio Network Controller
RRM	Radio Resource Management
RS	Resource Status
RT	Real Time
SAE	3GPP System Architecture Evolution
SGSN	Serving GPRS Support Node
TRX	Transceiver
TSA	Transport Service Availability
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunication System
UPE	User Plane Entity
UTRAN	Universal Terrestrial Radio Access Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

REFERENCES

[0069]

[1] http//www.ambient.networks.org

[2] N. Niebert, A. Schieder, H. Abramowicz, G. Malmgren, J. Sachs, U. Horn, C. Prehofer, and H. Karl. Ambient Networks - An Architecture for Communication Networks Beyond 3G. IEEE Wireless Communications, 11(2):14-21, Apr. 2004.

[3] Deliverable D-1.5, "AN Framework Architecture", December 2005.

[4] P. Magnusson, F. Berggren, I. Karla, R. Litjens, F. Meago, H. Haitao, R. Veronesi, "Multi-radio resource management for communication networks beyond 3G,". IEEE 62nd VTC (2005).

Claims

1. Radio resource management method in a mobile radio communication network employing different radio access technologies (UTRAN, GERAN, LTE, WiMAX) that overlap over a geographic area subdivided into cells belonging to the domains of respective controllers (RNC, BSC, E-NodeB, BS), including the following steps carried out by every controller for each controlled cell:

   d) calculating a transport service availability information element, called hereafter MUB, describing the availability of transport services in terms of maximum user bitrate that can currently be allowed to each transport service, separately for uplink and downlink, needed to plan usage of radio resources in the current and neighbouring cells, such as for handovers, cell reselections and new service setups;
   e) including said MUB information elements into management messages forwarded to the other controllers, either of the same or different technologies;
   f) checking said MUB information elements coming from the other controllers (BSC, RNC, E-NodeB, BS) in order to decide on the most suited target cell, among the current and neighbouring cells, for resource management issues such as handover, cell reselection, and new service setup;

   characterised in that said calculating step a) includes in its turn the following steps executed for each implemented service **characterised by** service type and high/low priority:

   a1) calculating an available capacity for a given service by taking a normalised capacity accessible to said service and by subtracting to it a normalized load of said service and of any other service that cannot be pre-empted by said service;
   a2) calculating a MUBN parameter for said service as the minimum between said available capacity and the maximum capacity MAXUB allowed to the single user for said service as a configuration setting;

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 841

a3) calculating a quantized representation MUB of the MUBN for said service for transmission over digital transmission means.

2. The method of claim 1, **characterized in that** said calculating step a) further includes for said service the steps of:

a4) calculating a parameter QN associated to MUB for said service and describing the number of available services of bitrate MUBN as the ratio between the available capacity and MUBN;
a5) calculating a parameter Q associated to MUB for said service as a quantized representation of QN for transmission over digital transmission means.

3. The method of claim 1, **characterized in that** in said step a1) the accessible capacity is either:

- all capacity accessible to the given service type for the highest service priority of said service or
- a percentage of all capacity accessible to the given service type according to a respective load threshold set for lower service priorities.

4. The method of claim 1, **characterized in that** said step a1) further includes the steps of:

- calculating the capacity accessible to said service by taking the total fixed cell capacity and by subtracting to it any capacity reserved to other services;
- considering the load of any other service that cannot be pre-empted by said service only in the portion of allocation into the capacity accessible to said service.

5. The method of claim 1, **characterized in that** said step a1) further includes subtracting the capacity allocated for control signalling in the portion of allocation into the capacity accessible to said service.

6. The method of claim 1, **characterized in that** said step a1) further includes considering the load of said service and of any other service that cannot be pre-empted by said service only in the portion required for providing a guaranteed Quality of Service, excluding any surplus resources currently given to said services.

7. The method of claim 1, **characterized in that** in said step a1) further includes using a conversion factor for translating normalised values of available capacity in net user bitrate indications of the same available capacity.

8. The method of claim 1, **characterized in that** in said step a2) further includes dynamically set in time the MAXUB as a function of the available capacity for the same service.

9. The method of claim 4, **characterized in that** further includes dynamically set in time said reserved capacities according to policies, current resource usage, resource bookings.

10. The method of claim 3 and 4, **characterized in that** further includes setting load thresholds on the reserved capacities for limiting access to the same capacities to a related portion, limiting **in that** the capacity accessible for lower service priorities.

11. The method of any claim from 1 to 10, **characterized in that** said MUB concerns conversational circuit-switched services.

12. The method of any claim from 1 to 10, **characterized in that** said MUB concerns Enhanced GPRS streaming services.

13. The method of any claim from 1 to 10, **characterized in that** said MUB concerns non-real-time GPRS services.

14. The method of any claim from 1 to 10, **characterized in that** said MUB concerns non-real-time Enhanced GPRS services.

15. The method of any claim from 1 to 10, **characterized in that** said MUB concerns low priority services.

16. The method of any claim from 1 to 10, **characterized in that** said MUB concerns high priority services.

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 842

17. The method of claim 1, **characterized in that** when a cell is evaluated as a potential target for a given service, said checking step c) includes in its turn the following steps:

c1) selecting for said cell the MUB information corresponding to said service;
c2) checking if the MUB information indicates the availability of the required bitrate for said service, in which case the cell is a suitable target cell.

18. The method of claim 2, **characterized in that** when two or more cells are compared as a potential target cells for a given service, said checking step c) includes in its turn the following steps:

c1) selecting for said cells the MUB information corresponding to said service;
c2) checking if the MUB information indicates the availability of the required bitrate for said service, in which case the cells satisfying this requirement are suitable target cells;
c3) checking the Q information element associated to said MUB information of different suitable target cells and selecting the cell with highest Q as the best target cell.

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 843

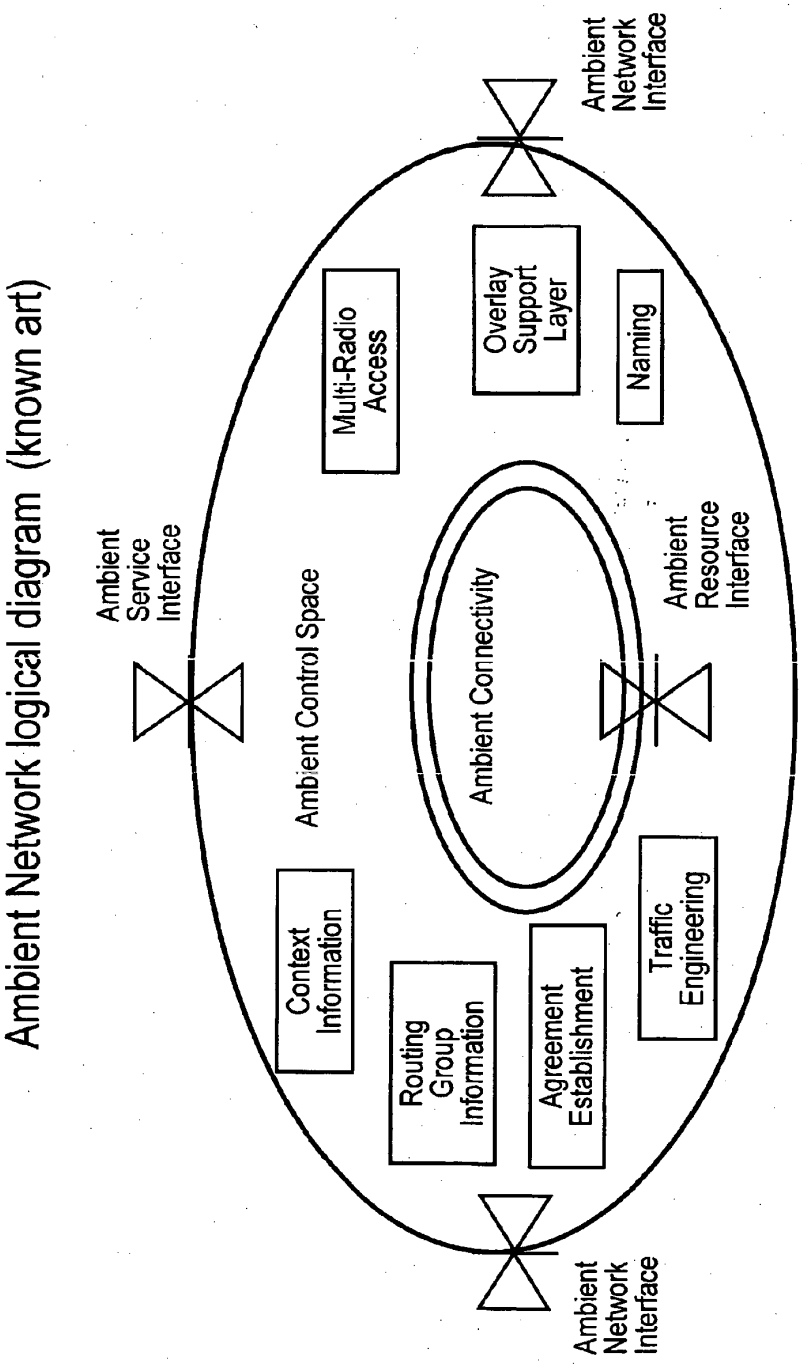


FIG. 1

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 844

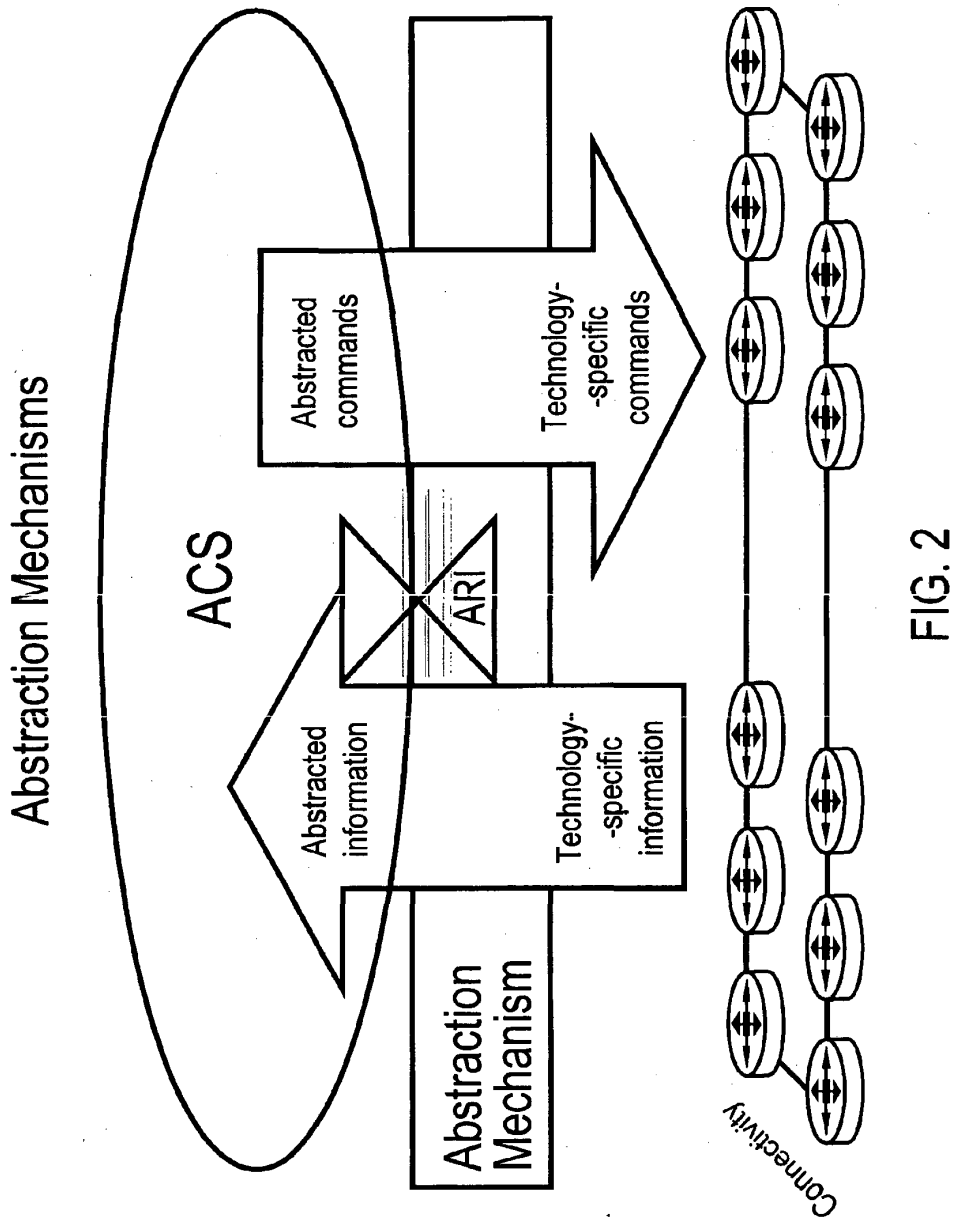


FIG. 2

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 845

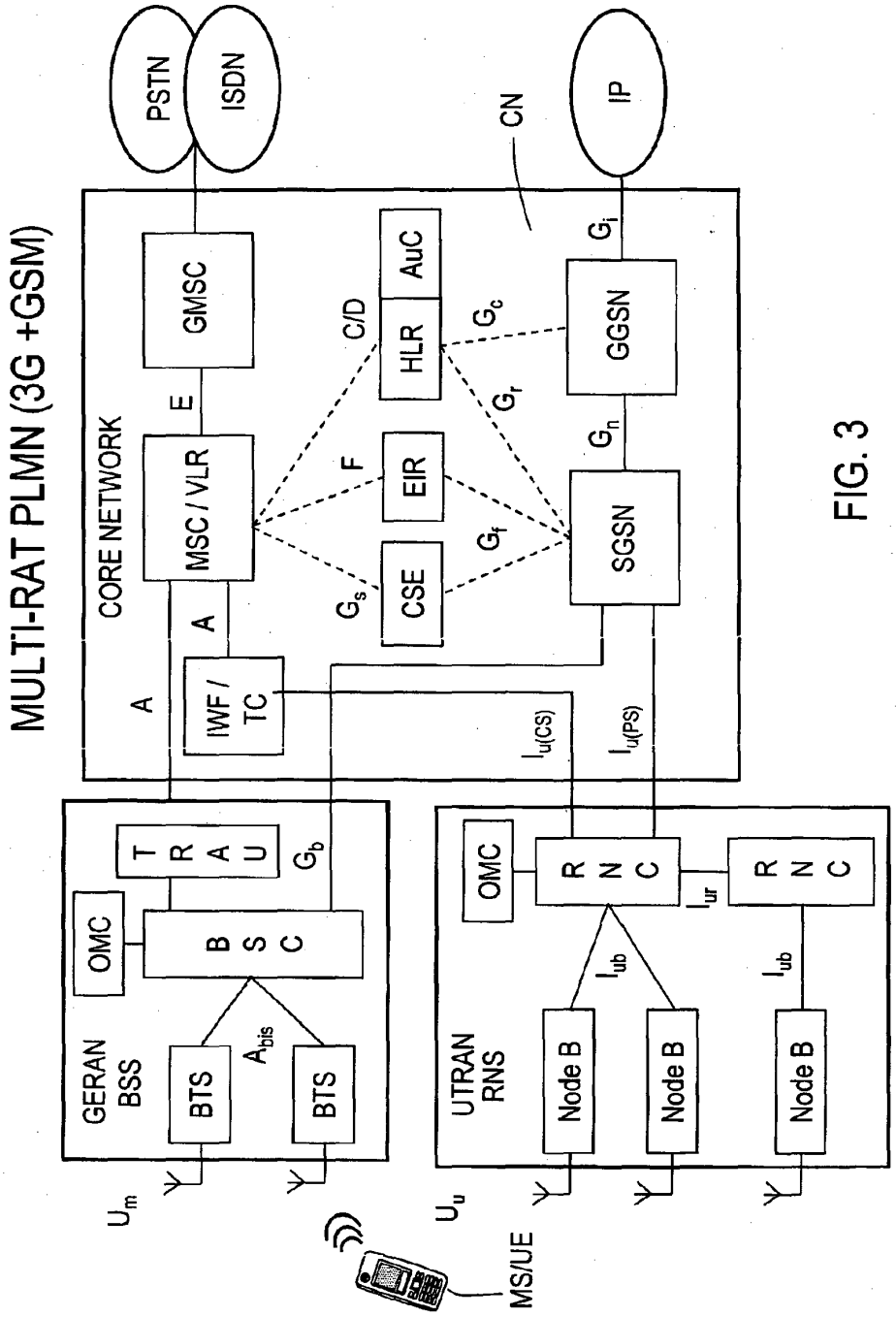


FIG. 3

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 846

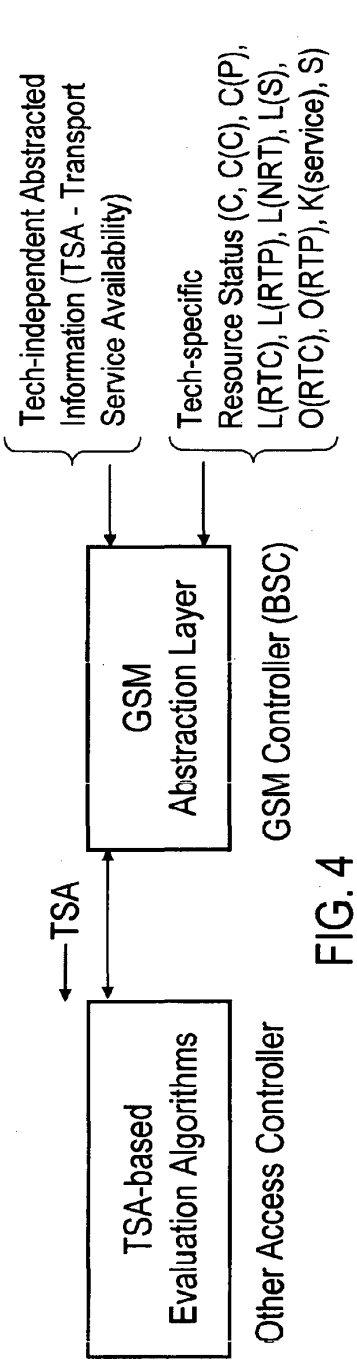


FIG. 4

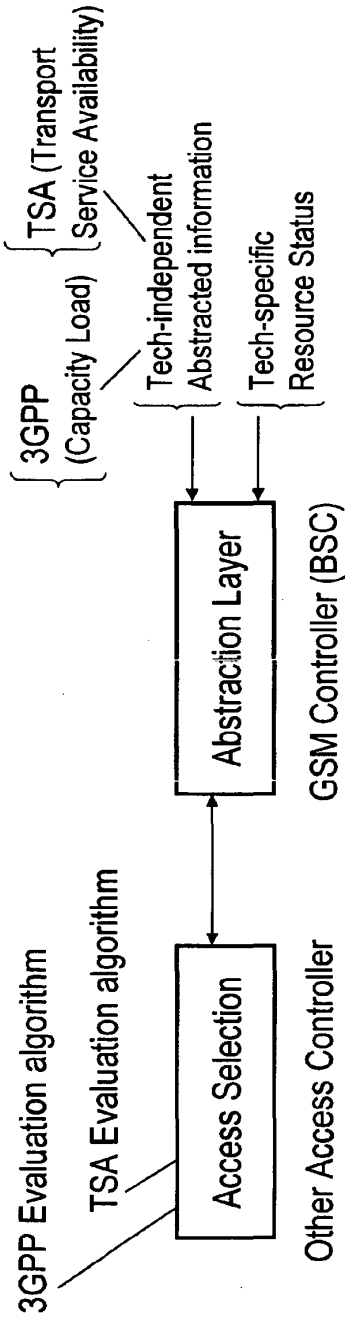


FIG. 5

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 847

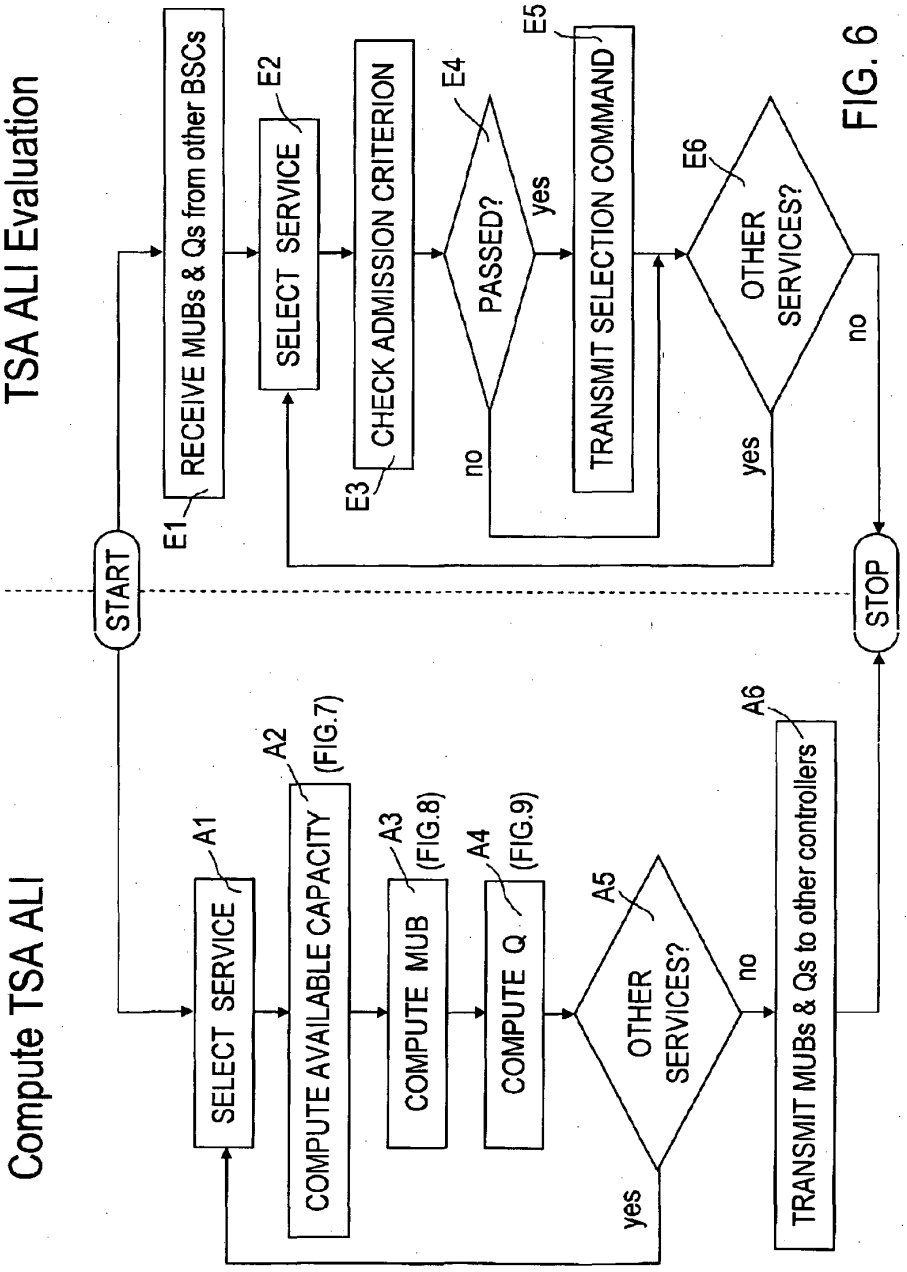


FIG. 6

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 848

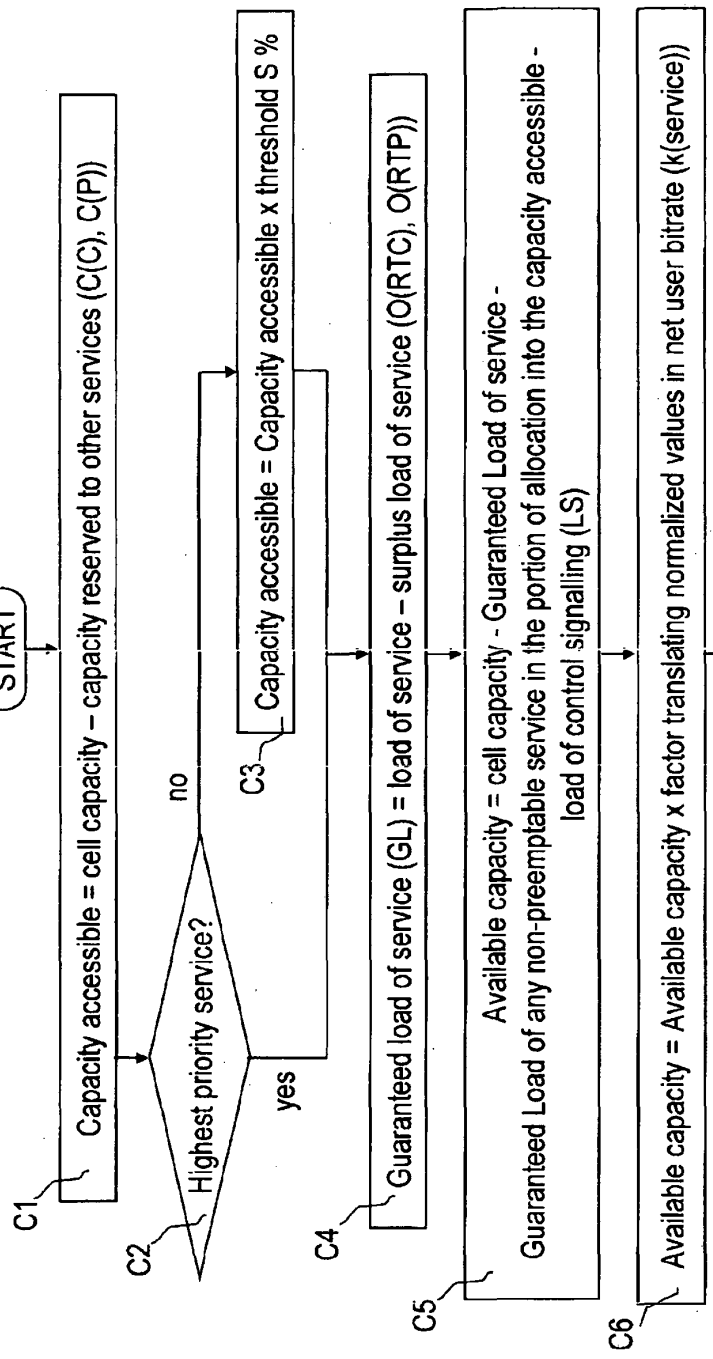


FIG. 7

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 849

FIG. 8

FIG. 9

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 850

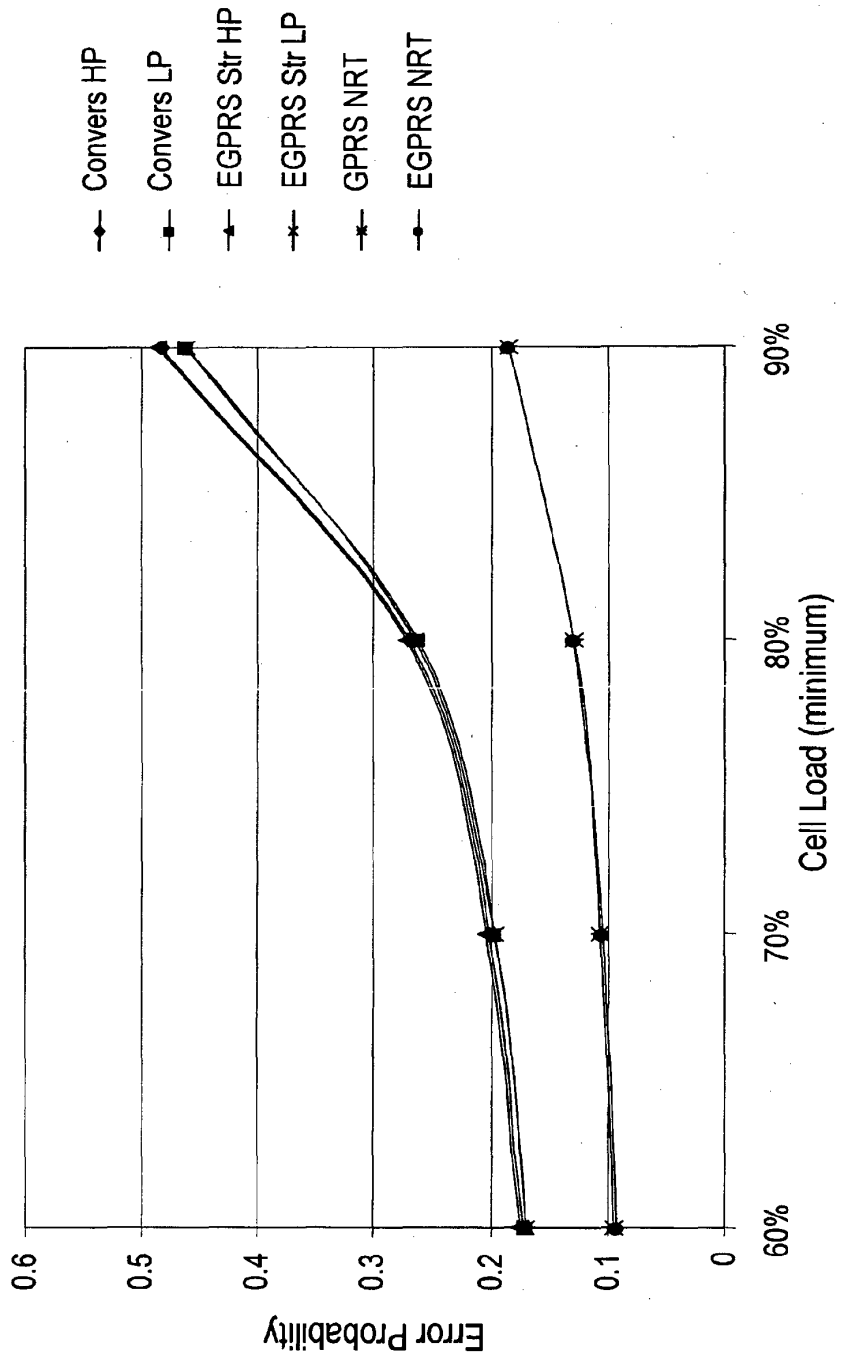


FIG. 10

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 851

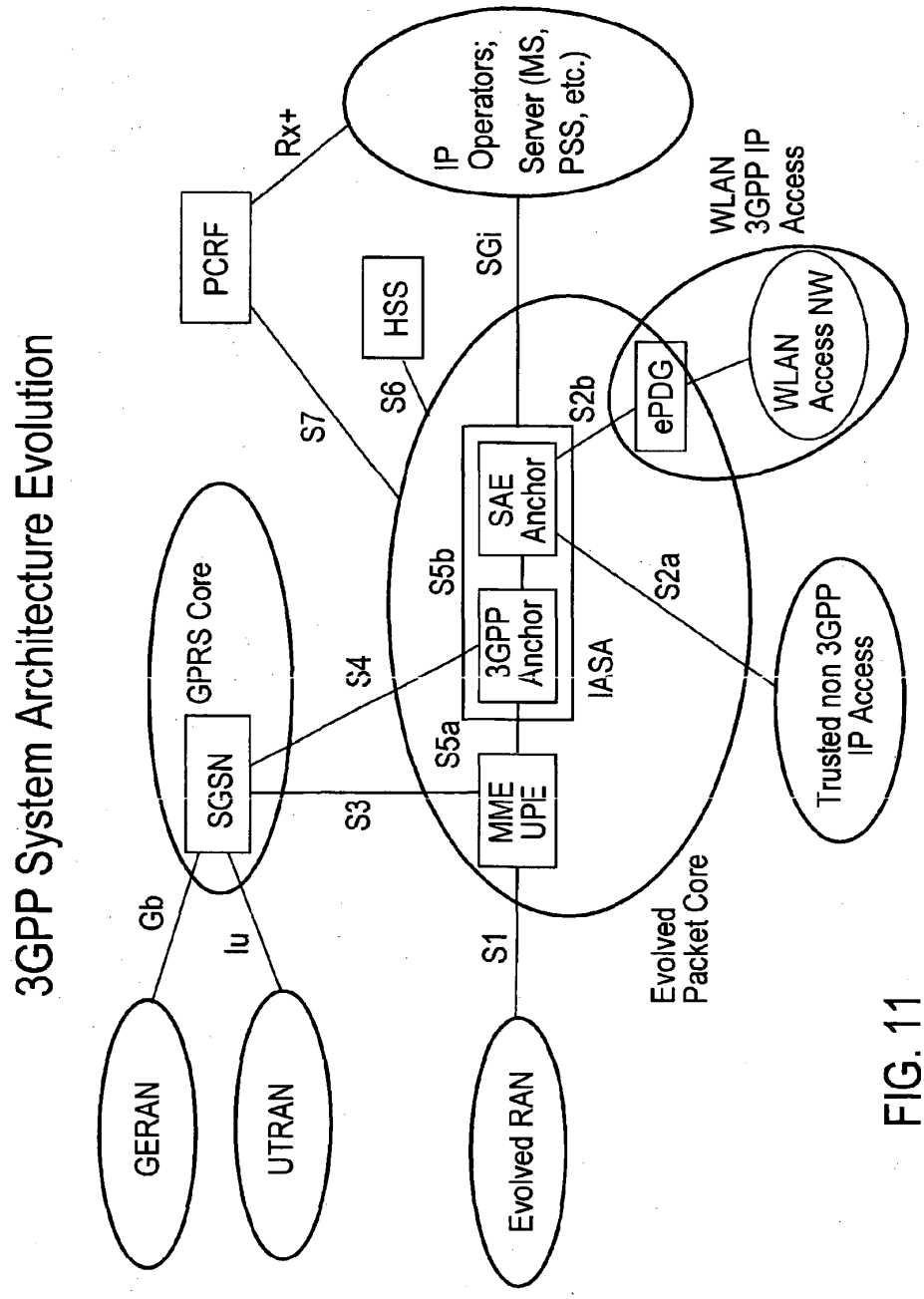


FIG. 11

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 852

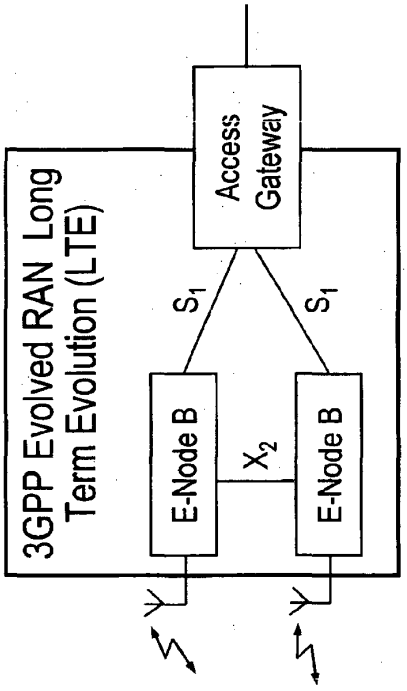


FIG. 12

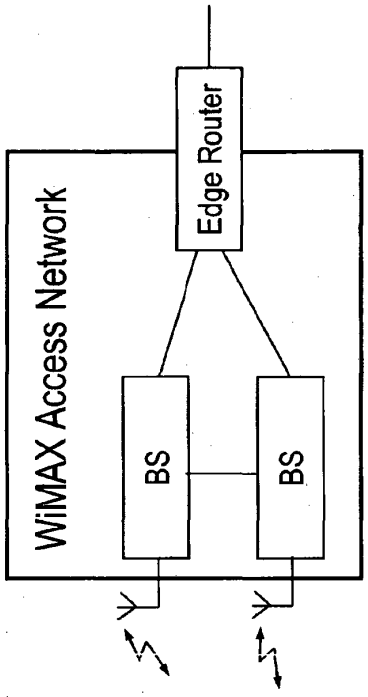


FIG. 13

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 853

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 42 5527

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	EP 1 503 606 A (SIEMENS MOBILE COMM SPA [IT]) 2 February 2005 (2005-02-02) * abstract; claims 1-21 *	1-18	INV. H04L12/56
Y	US 6 804 222 B1 (LIN WEI [US] ET AL) 12 October 2004 (2004-10-12) * abstract * * column 12, line 41 - column 13, line 11 * -----	1-18	
A	US 2003/117951 A1 (WIEBE MARVIN JAKE [CA] ET AL) 26 June 2003 (2003-06-26) * abstract * -----	1-18	
A	EP 1 420 604 A (SIEMENS MOBILE COMM SPA [IT] SIEMENS SPA ITALIANA [IT]) 19 May 2004 (2004-05-19) * abstract * * claims 1-10 * -----	1-18	
			TECHNICAL FIELDS SEARCHED (IPC) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	13 February 2008	Wolf, William

CATEGORY OF CITED DOCUMENTS

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

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

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 854

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 42 5527

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.

13-02-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1503606 A	02-02-2005	CN 1582054 A	16-02-2005
		US 2005026616 A1	03-02-2005
US 6804222 B1	12-10-2004	US 2005041670 A1	24-02-2005
US 2003117951 A1	26-06-2003	EP 1330060 A2	23-07-2003
		JP 2003229902 A	15-08-2003
EP 1420604 A	19-05-2004	AT 341170 T	15-10-2006
		DE 60215026 T2	16-05-2007
		EP 1657862 A1	17-05-2006

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 855

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

- EP 1503606 A1 **[0012] [0013]**

Non-patent literature cited in the description

- **N. NIEBERT ; A. SCHIEDER ; H. ABRAMOWICZ ; G. MALMGREN ; J. SACHS ; U. HORN ; C. PREHOFER ; H. KARL. AMBIENT NETWORKS.** An Architecture for Communication Networks Beyond 3G. *IEEE Wireless Communications,* April 2004, vol. 11 (2), 14-21 **[0069]**
- *Deliverable D-1.5, "AN Framework Architecture,* December 2005 **[0069]**
- **P. MAGNUSSON ; F. BERGGREN ; I. KARLA ; R. LITJENS ; F. MEAGO ; H. HAITAO ; R. VERONESI.** Multi-radio resource management for communication networks beyond 3G. *IEEE 62nd VTC,* 2005 **[0069]**

BNSDOCID: <EP_____2026514A1_I_>

IPR2025-01572
Apple EX1002 Page 856

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 942 698 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.07.2008 Bulletin 2008/28

(51) Int Cl.:
H04Q 7/38 *(2006.01)*

(21) Application number: **08250053.9**

(22) Date of filing: **07.01.2008**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Designated Extension States:
AL BA MK RS

(30) Priority: **07.01.2007 US 879318 P**
22.06.2007 US 821598
22.06.2007 US 821597

(71) Applicant: **Apple Inc.**
Cupertino, CA 95014 (US)

(72) Inventors:
- **Gautier, Patrice**
  San Francisco, CA 94121 (US)
- **Shimizu, Debbie**
  San Jose, CA 95126 (US)
- **Anderson, Alexandrea**
  Clovis, CA 93611 (US)
- **Cue, Eddy**
  Los Altos, CA 94024 (US)
- **Gromek, Monika**
  Oakland, CA 94607 (US)
- **Kondrk, Robert, H.**
  San Francisco, CA 94107 (US)

(74) Representative: **Alton, Andrew**
Urquhart-Dykes & Lord LLP
Tower North Central
Merrion Way
Leeds LS2 8PA (GB)

(54) Method and system for mobile device activation

(57) Methods, systems and graphical user interfaces that facilitate activation of mobile devices, such as communication devices or multi-function devices, via computers are disclosed. According to one embodiment, activation of a mobile device with respect to a wireless service provider can be performed by users through use of a computer (e.g., personal computer) that communicate with a remotely located activation server. According to another embodiment, graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices.

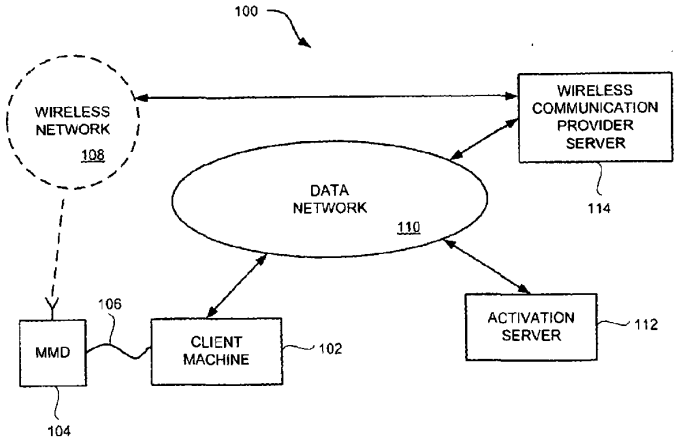


FIG. 1

EP 1 942 698 A1

Description

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention relates to mobile electronic devices and, more particularly, to activation of mobile electronic devices having wireless communication capabilities.

Description of the Related Art

[0002] Mobile phones are often used by individuals on a personal basis. When a mobile phone is newly acquired, the wireless network infrastructure (e.g., cellular phone network) of the appropriate wireless carrier or service provider needs to be setup to work with the mobile phone. Mobile phone setup is principally done at retail establishments that sell mobile phones and wireless service plans. Alternatively, mobile phones can be configured at a manufacturing or distribution site or at a service center. Unfortunately, however, mobile phone setup is time consuming and restrictive to consumers. Additionally, once a mobile phone and service plan have been setup for a consumer, the wireless network needs to be informed of the mobile phone and the mobile phone thereafter needs to register with the wireless network whenever being used. Registration requires a location update request be sent from the mobile phone to the wireless network. In the case of initial phone setup, since location update is triggered on power-up, typically the person configuring the mobile phone would be required to power-off and then power-on the mobile phone to render it active on the wireless network. There is thus a need to avoid the various inconveniences and inefficiencies of conventional mobile phone setup.

SUMMARY OF THE INVENTION

[0003] The invention pertains to methods, systems and graphical user interfaces that facilitate setup or activation of mobile devices, such as communication devices or multi-function devices, via computers. According to one embodiment, activation of a mobile device with respect to a wireless service provider can be performed by users through use of a computer (e.g., personal computer) that communicate with a remotely located activation server. According to another embodiment, graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices.

[0004] The invention can be implemented in numerous ways, including as a method, system, device, apparatus, graphical user interface, or computer readable medium. Several embodiments of the invention are discussed below.

[0005] As a computer-implemented method for activating wireless network service for an electronic device through use of a host device, where the electronic device is associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least the acts of: receiving device information from the electronic device when the electronic device is attached to the host device; acquiring customer information pertaining to the customer; receiving a service plan selection from the customer; receiving billing information for payment of the service plan; and initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider. The wireless service account being activated can be based on the customer information, the service plan and the billing information.

[0006] As a computer-implemented method for activating an electronic device for wireless network service through use of a host device, where the electronic device is associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least the acts of: receiving device information from the electronic device while the electronic device is attached to the host device; acquiring customer information pertaining to the customer; offering the user one or more service plans; receiving a user selection of one of the service plans; and receiving billing information for payment of the selected service plan.

[0007] As a computer-implemented method for activating an electronic device for wireless network service from a host device, where the electronic device is associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least the acts of: receiving device information from the electronic device when the electronic device is attached to the host device; determining whether the electronic device has already been activated based on the device information; and automatically initiating activation of the electronic device when it is determined that the electronic device has not already been activated.

[0008] As a graphical user interface to assist an end user in activating an account for an electronic device having wireless communication capabilities, where the account is with respect to a wireless service provider providing wireless network service, one embodiment of the invention can, for example, include at least a plurality of displayable pages that are presented on a display device associated with a host computer. The displayable pages can, for example, include: an end user status page to facilitate selection of a type of activation; a service plan selection page to facilitate selection of a service plan for the wireless network service; a media account page for a media account associated with an online media store so that a user can create a new media account or login to an existing media account; an end user information entry page to facilitate entry of end user information; a billing information page to facilitate entry of billing infor-

IPR2025-01572
Apple EX1002 Page 858

mation for one or both the user media account and a wireless account; a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider; and/or an activation page to inform the end user of activation information.

[0009] As a computer-implemented method for activating an electronic device for wireless network service, where the electronic device is associated with a customer of a wireless service provider associated with the wireless network service, one embodiment can, for example, include at least the acts of: informing an activation server of an electronic device having wireless communication device that is to be activated for wireless network service; displaying a customer status page to facilitate selection of a type of activation; specifying to the activation server a type of activation desired by the customer; displaying a service plan selection page to facilitate selection of a service plan for the wireless network service; informing the activation server of a selected service plan; displaying a customer account page to facilitate login to or creation of a user media account with an online media store; providing account information for the user media account for the customer; displaying a customer information entry page; providing customer information to the activation server; displaying a billing information page to facilitate entry of billing information for one or both the user media account and a wireless account; informing the activation server of the billing information; displaying a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider; informing the activation server of acceptance of the legal agreements; displaying an information review page; informing the activation server of approval of the information provided on the information review page; displaying an activation completion page; and displaying a device preference page to assist the customer with setting one or more preferences or options to be applied to the operation of the electronic device.

[0010] As a computer readable medium including at least computer executable program code tangibly embodied therein for activating wireless network service for an electronic device through use of a client computing device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least: computer program code for receiving device information from the electronic device when the electronic device is attached to the host device; computer program code for acquiring customer information pertaining to the customer; computer program code for receiving a service plan selection from the customer; computer program code for receiving billing information for payment of the service plan; and computer program code for initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider.

[0011] As a computer readable medium including at least computer executable program code tangibly embodied therein for activating an electronic device for wireless network service through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, one embodiment can, for example, include at least: computer program code for receiving device information from the electronic device while the electronic device is attached to the host device; computer program code for acquiring customer information pertaining to the customer; computer program code for offering the user one or more service plans; computer program code for receiving a user selection of one of the service plans; and computer program code for receiving billing information for payment of the selected service plan.

[0012] Other aspects and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying drawings which illustrate, by way of example, the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

[0014] FIG. 1 is a block diagram of an activation system according to one embodiment of the invention.

[0015] FIG. 2A is a flow diagram of a system activation process according to one embodiment of the invention.

[0016] FIG. 2B is a flow diagram of a setup process according to one embodiment of the invention.

[0017] FIG. 3 is a flow diagram of a device operational process according to one embodiment of the invention.

[0018] FIG. 4 is a flow diagram of a device operation process according to another embodiment of the invention.

[0019] FIG. 5 is a system state diagram according to one embodiment of the invention.

[0020] FIGs. 6A-6C are flow diagrams of a network service setup process according to one embodiment of the invention.

[0021] FIG. 6D is a flow diagram of an alternative portion of the network service setup process according to one embodiment of the invention.

[0022] FIG. 7 is a flow diagram of a network service setup process according to one embodiment of the invention.

[0023] FIGs. 8A-8C are flow diagrams of an activation process according to one embodiment of the invention.

[0024] FIG. 9 is a flow diagram of an activation process according to another embodiment of the invention.

[0025] FIG. 10 is a flow diagram of an activation process according to another embodiment of the invention.

[0026] FIG. 11 is a flow diagram of an activation process according to another embodiment of the invention.

[0027] FIGs. 12A-12C are flow diagrams of a mobile

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 859

device provisioning process according to one embodiment of the invention.

[0028] FIG. 13 is a screen shot of an exemplary initial registration page according to one embodiment of the invention.

[0029] FIG. 14 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0030] FIG. 15 is a screen shot of an exemplary screen shot of a mobile number transfer page.

[0031] FIG. 16 is a screen shot of an exemplary screen shot of a landline number transfer page.

[0032] FIG. 17A and 17B are screen shots of an exemplary service plan selection page according to one embodiment of the invention.

[0033] FIG. 18 is a screen shot of an exemplary customer account page according to one embodiment of the invention.

[0034] FIG. 19 is a screen shot of a customer information entry page according to one embodiment of the invention.

[0035] FIG. 20 illustrates an exemplary billing information page according to one embodiment of the invention.

[0036] FIG. 21A is an exemplary screen shot of a first terms and conditions page according to one embodiment of the invention.

[0037] FIG. 21B is an exemplary screen shot of a second terms and conditions page according to one embodiment of the invention.

[0038] FIG. 22 is a screen shot of an exemplary review information page according to one embodiment of the invention.

[0039] FIG. 23 is an exemplary screen shot of a setup completion page according to one embodiment of the invention.

[0040] FIG. 24A is an exemplary screen shot of a setup completion page according to another embodiment of the invention.

[0041] FIG. 24B is an exemplary screen shot of a setup completion page according to still another embodiment of the invention.

[0042] FIG. 25 is an exemplary screen shot of a device preference page according to one embodiment of the invention.

[0043] FIG. 26 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0044] FIG. 27 is a screen shot of an exemplary account information page according to one embodiment of the invention.

[0045] FIG. 28 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0046] FIG. 29 is a screen shot of an exemplary account information page according to one embodiment of the invention.

[0047] FIG. 30 is a screen shot of an exemplary account type selection page according to one embodiment of the invention.

[0048] FIG. 31 is a screen shot of an exemplary customer status page according to one embodiment of the invention.

[0049] FIG. 32 is a screen shot of an exemplary account type selection page according to one embodiment of the invention.

[0050] FIG. 33 is a screen shot of an exemplary prepayment requirement page.

[0051] FIG. 34 is a block diagram of a mobile multi-function device according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0052] The invention pertains to methods, systems and graphical user interfaces that facilitate setup or activation of mobile devices, such as communication devices or multi-function devices, via computers. According to one embodiment, activation of a mobile device with respect to a wireless service provider can be performed by users through use of a computer (e.g., personal computer) that communicate with a remotely located activation server. According to another embodiment, graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices.

[0053] Embodiments of the invention are discussed below with reference to FIGs. 1 - 34. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the invention extends beyond these limited embodiments.

[0054] FIG. 1 is a block diagram of an activation system 100 according to one embodiment of the invention. The activation system 100 includes a client machine 102. The client machine 102 is, for example, a computing device, such as a personal computer. The client machine 102 can also be referred to as a host device. A mobile multi-function device 104 can be connected (e.g., temporarily connected) to the client machine 102. In one implementation, the mobile multi-function device 104 can be connected to the client machine 102 over a cable 106. As an example, the cable 106 can pertain to a peripheral bus (e.g., USB) connection. In another implementation, the mobile multi-function device 104 can connect to the client machine 102 over a wireless connection. The mobile multi-function device 104 operates to support a plurality of different functions. For example, the mobile multi-function device 104 can operate as a media playback device, such as an MP3 player, video player, game player, etc. In addition, the mobile multi-function device 104 can support wireless voice communications through a wireless network 108. The wireless voice communications through the wireless network 108 can enable a user of the mobile multi-function device to communicate with users of other mobile multi-function devices or other communication devices. Similarly, the mobile multi-function device 104 can support wireless data exchange (e.g.,

IPR2025-01572
Apple EX1002 Page 860

SMS messages) through the wireless network 108. Although FIG. 1 illustrates one client machine 102 and one mobile multi-function device 104, it should be noted that the activation system 100 can have multiple client machines 102 and multiple mobile multi-function devices 104. In addition, one or more of the mobile multi-function devices can connect to one or more client machines. In one implementation, the wireless network 108 can represent a cellular telephone network. In another implementation, the wireless network 108 can represent a local or regional wireless network (e.g., WiFi, WiMax). In still another implementation, the wireless network 108 can represent multiple wireless networks.

[0055] The activation system 100 also illustrates a data network 110. The data network is, for example, a local area network, a wide area network, or a global network, such as the Internet. The client machine 102 can couple to the data network 110. In addition, the activation system 100 includes an activation server 112 and a wireless communication provider server 114. In order to activate the mobile multi-function device 104, the mobile multi-function device 104 interacts with the activation server 112. To do so, the mobile multi-function device 104 communicates with the client machine 102 and the client machine 102 in turn communicates with the activation server 112 through the data network 110. In this regard, the activation server 112 can coordinate and control activation of the mobile multi-function device 104. In addition, the activation server 112 can communicate with the wireless communication provider server 114 so that an appropriate account to be utilized by the mobile multi-function device 104 can be established by the wireless communication provider that is operating on the wireless network 108.

[0056] FIG. 2A is a flow diagram of a system activation process 200 according to one embodiment of the invention. The system activation process 200 concerns activation of a mobile multi-function device (MMD). The system activation process 200 begins with a mobile multi-function device being obtained 202. For example, a user can obtain 202 a mobile multi-function device at a retail location or by mail order. In this embodiment, when the mobile multi-function device is obtained 202, it is not activated for use with any wireless network. As a result, the mobile multi-function device needs to go through an activation process in order to operate. In this regard, after the mobile multi-function device is obtained 202, a service plan and a payment arrangement need to be setup 204. After the service plan and payment arrangement have been successfully setup 204, the mobile multi-function device can be enabled 206. In addition, the mobile multi-function device can be registered with a network, namely, a wireless network. Here, the registration 208 with the network is performed to permit the mobile multi-function device to be utilized on the network.

[0057] Following successful enabling 206 and registration 208, the mobile multi-function device can operate 210 with or without utilization of the network. In this regard, since the mobile multi-function device supports multiple functions, the mobile multi-function device can be utilized in a non-network manner, such as playing local games, displaying local data, playing music from local storage, viewing local pictures, viewing locally stored electronic mail, etc. However, if the user of the mobile multi-function device desires to utilize the network (e.g., make or receive voice calls or electronic messages), network access is permitted in accordance with the service plan that has been setup 204, provided that the registration 208 was successful and provided that the network is available.

[0058] Once the mobile multi-function device is enabled 206 some or all of the functions or operations supported by the mobile multi-function device can be utilized. In one embodiment, once enabled 206, the mobile multi-function device can be utilized for all non-network functions or operations available from the mobile multi-function device, with network functions or operations becoming available following registration at block 208. In another embodiment, functions or operations of the mobile multi-function device can be prevented or restricted until completion of initial (i.e., first time) registration at block 208 at which point all functions or operations available from the mobile multi-function device can be utilized. In still another embodiment, certain, non-network functions or operations of the mobile multi-function device can be available even prior to the mobile multi-function device being enabled 206.

[0059] FIG. 2B is a flow diagram of a setup process 250 according to one embodiment of the invention. The setup process 250 operates to setup a service plan and/or payment arrangement with respect to one or more service providers. The setup process 250 is, for example, suitable for use as the setup 204 of a service plan and payment arrangement illustrated in FIG. 2A.

[0060] The setup process 250 retrieves 252 device information. Typically, the device information is retrieved 252 from the device itself. For example, the device can be referred to as a mobile multi-function device. Customer information can also be acquired 254, such as from the customer. The customer information can be acquired 254 so that the service provider can receive information regarding the customer that seeks to activate the mobile multi-function device. A service plan for the device is also set 256. The customer can be offered one or more service plans depending upon various different criteria, including customer's location, customer's credit history, customer's current service provider, etc. A service plan as used herein can also be referred to as a rate plan. Once a service plan to be utilized with the customer has been set 256, a billing account can be setup 258. The building account serves to facilitate billing the customer for the services provided by the service plan. Typically, the customer is billed monthly for the service plan. The setup 258 of the billing account acquires all the necessary information for billing the customer. As one example, the billing account can utilize a credit card whereby the cus-

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 861

tomer is billed monthly via the credit card for the service plan. Subsequently, the customer account can be activated 260. In this regard, the setup process 250 can communicate with a computing device (e.g., activation server 112) associated with a service provider to activate a customer account so that the customer can utilize the mobile multi-function device with the at least one service provider in accordance with the service plan. The service provider is, for example, a wireless (communications) service provider. Additionally, an account with another service provider, such as an online media store, can be established. Following the block 260, the setup process 250 ends and subsequent processing can continue at block 206 of the system activation process 200 illustrated in FIG. 2A.

[0061] FIG. 3 is a flow diagram of a device operational process 300 according to one embodiment of the invention. The device operational process 300 is, for example, processing associated with a mobile multi-function device, such as the mobile multi-function device 104 illustrated in FIG. 1.

[0062] The device operational process 300 can begin when the mobile multi-function device is powered on. Hence, a decision 302 determines whether the mobile multi-function device has been powered on. When the mobile multi-function device has not been powered on, the device operational process 300 is not performed. On the other hand, when the decision 302 determines that the mobile multi-function device has been powered on, a decision 304 can determine whether the mobile multi-function device has been enabled. Here, it is assumed that the mobile multi-function device performing the device operational process 300 may or may not have been enabled to operate. Hence, when the decision 304 determines that the mobile multi-function device has not been enabled, the mobile multi-function device is eligible to operate 306 in a limited use mode. As an example, in the limited use mode, the mobile multi-function device can permit emergency communications (e.g., emergency telephone calls). However, the limited use mode may prevent other operations of the mobile multi-function device. For example, if the mobile multi-function device provides media playback or network browsing, then when in the limited use mode, media playback and/or network browsing can be prevented (or limited). In one implementation, while in the limited use mode, the mobile multi-function device can prevent all other operational uses except emergency communications.

[0063] On the other hand, when the decision 304 determines that the mobile multi-function device is enabled, the mobile multi-function device can operate in a full use mode. Following the blocks 306 and 308, a decision 312 can determine whether the mobile multi-function device is to be powered off. When the decision 312 determines that the mobile multi-function device should not be powered off, the mobile multi-function device continues to operate in the previously established operational mode (e.g., limited use mode or full use mode). On the other hand, when the decision 312 determines that the mobile multi-function device should be powered off, the mobile multi-functional device is powered down 314. Following the block 314, the device operational process 300 can end.

[0064] FIG. 4 is a flow diagram of a device operation process 400 according to another embodiment of the invention. The device operational process 400 is, for example, processing associated with a mobile multi-function device, such as the mobile multi-function device 104 illustrated in FIG. 1.

[0065] The device operational process 400 begins with a decision 402. The decision 402 determines whether the mobile multi-function device has been powered on. When the decision 402 determines that the mobile multi-function device has not been powered on, the device operational process 402 awaits power on of the mobile multi-function device. Once the decision 402 determines that the mobile multi-function device has been powered on, the device operational process 400 is effectively invoked. Once the decision 402 determines that the mobile multi-function device has been powered on, a decision 404 determines whether the mobile multi-function device has been enabled.

[0066] When the decision 404 determines that the mobile multi-function device has not yet been enabled, the device operational process 400 places 406 the mobile multi-function device in an emergency mode. In the emergency mode, the mobile multi-function device is permitted to make emergency calls only. Next, a decision 408 determines whether the mobile multi-function device is to be powered off. When the decision 408 determines that the mobile multi-function device is not to be powered off, the device operational process 400 returns to repeat the decision 404 to again evaluate whether the mobile multi-function device has been enabled. In an alternative embodiment, when the decision 408 determines that the mobile multi-function device is not to be powered off, the device operation process 400 can remain in the emergency mode and simply repeat the decision 404 until powered off.

[0067] Alternatively, when the decision 404 determines that the mobile multi-function device has been enabled, the mobile multi-function device is placed 410 in an active mode. Registration with a wireless network can also be requested 412. In one embodiment, a location update request can be used to request 412 registration with the wireless network. A decision 414 determines whether the registration with the wireless network has been successful. When the decision 414 determines that the registration has been successful, the device operational process 400 permits 416 the mobile multi-function device to perform network and/or non-network operations. Next, a decision 418 determines whether the mobile multi-function device is to be powered off. When the decision 418 determines that the mobile multi-function device has not been powered off, the device operational process 400 returns to repeat the block 416 so that the

IPR2025-01572
Apple EX1002 Page 862

mobile multi-function device can continue to perform 416 network and/or non-network operations.

[0068] On the other hand, when the decision 414 determines that registration with the wireless network has not been successful, then the user of the multi-function device can be notified 422 that the network is unavailable. In one implementation, the notification 422 can be displayed on a display screen for one or both of the multi-function device or a client device connected thereto. Further, the mobile multi-function device can be operated to permit 424 non-network operations. A decision 426 can then determine whether the mobile multi-function device is to be powered off. When the decision 426 determines that the mobile multi-function device is not to be powered off, the device operational process 400 returns to repeat the block 424 so that non-network operations can continue to be performed 424.

[0069] When any of the decisions 408, 418 or 426 determine that the mobile multi-function device is to be powered off, the mobile multi-function device can be powered down 420. After the mobile multi-function device has been powered down, the device operational process 400 ends.

[0070] FIG. 5 is a system state diagram 500 according to one embodiment of the invention. The system state diagram 500 illustrates a plurality of states associated with system activation of a mobile multi-function device (MMD) according to one embodiment. At state 502, a mobile multi-function device is obtained. At state 504, following the state 502, the mobile multi-function device is powered-on. Next, at state 506, the mobile multi-function device is connected to a computer, (e.g., personal computer). Thereafter, at state 508, one or more accounts can be arranged. These accounts can pertain to an account with an online media store and/or an account with a wireless service provider. Next, at state 510, a service plan can be selected. Typically, the service plans are associated with a wireless service provider that is providing wireless network access for the mobile multi-function device. In addition, payment can be arranged at state 512. It should also be noted that states 510 and/or 512 could be part of the state 508.

[0071] Following state 512, at state 514, the mobile multi-function device can be enabled. Once enabled, the mobile multi-function device is able to be fully utilized. Subsequently, the mobile multi-function device can be registered with a network (e.g., wireless network) at state 516. The registration with the network enables the mobile multi-function device to send and receive calls with respect to the network. Optionally, it should be noted that following the state 504, in the event that the mobile multi-function device was previously enabled, the mobile multi-function device can transition directly to state 516. In any case, once the mobile multi-function device has been registered with the network at state 516, the mobile multi-function device can be utilized with the network at state 518. Following the state 518, the mobile multi-function device can be powered off at state 520. Also, following the state 514, the mobile multi-function device can be disconnected from the computer at state 522 or the mobile multi-function device can be powered off at state 524.

[0072] In an alternative embodiment, at state 514, the mobile multi-function device can be enabled for only certain functions or operations. In this manner, the mobile multi-function device can have its available functions or operations controlled such that available functions or operations can be available (and others restricted) at (i) pre-enablement, (ii) post-enablement, and (iii) post-registration.

[0073] As such, activation can include one or more of account activation, device activation (i.e., enablement), and network activation (i.e., network setup). In one embodiment, the states 508, 510 and 512 can be considered account activation, and the state 514 can be considered device activation. Following state 512 or state 514 and prior to 516, the network can be setup (i.e., network activation) to support the account for the mobile multi-function device being activated.

[0074] FIGs. 6A-6C are flow diagrams of a network service setup process 600 according to one embodiment of the invention. For example, with reference to FIG. 1, the network service setup process 600 is processing performed when the mobile multi-function device 104 is connected to the client machine 102 illustrated in FIG. 1 so that interaction with the activation server 112 can be performed to setup service for the mobile multi-function device 104.

[0075] The network service setup process 600 can begin with a decision 602 that determines whether the mobile multi-function device is attached to the client machine (e.g., personal computer). When the decision 602 determines that the mobile multi-function device is not attached, then the network service setup process 600 is not performed. On the other hand, when the decision 602 determines that the mobile multi-function device is attached, the network service setup process 600 can be performed. In one embodiment, the network setup process 600 can be automatically initiated where the mobile multi-function device is attached to the client machine.

[0076] When the network setup process 600 is performed, mobile multi-function device (MMD) information is received 604 from the mobile multi-function device. Next, a decision 605 determines whether a user activation request has been received. When the decision 605 determines that a user activation request has not been received, the network service setup process 600 can await a user activation request. A user can request activation of the mobile multi-function device. In one example, the user can specify whether the activation of the mobile multi-function device is to be associated with a new account or an existing account. On the other hand, when the decision 605 determines that a user activation request has been received, a decision 606 can then determine whether the mobile multi-function device is to be subject to an existing account. The decision 606 can be based on the user activation request which can indicate

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 863

whether the activation of the mobile multi-function device is to be associated with a new account or an existing account. When the decision 606 determines that the mobile multi-function device is not subject to an existing account, account setup information is requested 608. The account setup information is information used to setup a new account. The account setup information can, for example, be provided by user. A decision 610 then determines whether the account setup information has been received. When the decision 610 determines that the account setup information has not yet been received, the network service setup process 600 awaits such information. Once the decision 610 determines that the account setup information has been received, a user account can be setup 612. The user account can pertains to a user account with a wireless service provider, an online media store, and/or some other account. The user account contains information concerning the user and often includes personal information and financial information.

[0077] On the other hand, when the decision 606 determines that an existing account is associated with the mobile multi-function device, authentication information can be requested 614. A decision 616 can then determine whether the authentication information has been received. When the decision 616 determines that the authentication information has not yet been received, the network service setup process 600 can await such information. Alternatively, when the decision 616 determines that the authentication information has been received, a decision 618 can determine whether the user is authenticated for access to the existing account. When the decision 618 determines that the user has not been authenticated, an error indication 620 can be provided. Following the block 620, the network service setup process 600 can end with network setup not being completed.

[0078] Following the block 612 or following the decision 618 when the user has been properly authenticated, the user can be offered 622 one or more service plans. In one embodiment, the one or more service plans being offered 622 can depending on a credit evaluation (e.g., credit score) for the user. For example, a user having poor credit can be only offered service plans that require prepayment. A decision 624 then determines whether a plan has been selected but the user. When the decision 624 determines that a plan has not yet been selected, the network service setup process 600 awaits such a selection. Once the decision 624 determines that a plan has been selected, a decision 628 determines whether a new account is being processed. When the decision 628 determines that a new account is being processed, setup of a billing account can be requested 630. However, when the decision 628 determines that an existing account is being processed, the block 630 can be bypassed. The request 630 can include payment information, such as payment information provided by the user. In one embodiment, the network setup process 600 already received or has access to the payment information to be used for the account. As one example, the account setup information can include the billing account information. In another embodiment, the network setup process 600 can request and receive the payment information prior to the request 630. When the decision 628 determines that payment information has not yet been received, the network service setup process 600 can await receipt of the payment information. Once the decision 628 determines that the payment information has been received, setup of a billing account can be requested 630.

[0079] Thereafter, activation of the account for the user can be requested 631. A decision 632 can then determine whether activation confirmation and phone number for the account being established have been received. When the activation confirmation and phone number have not been received, the network service setup process 600 can await such information. Alternatively, when the decision 632 determines that the activation confirmation and phone number have been received, the user can be informed 634 of successful account setup and the appropriate phone number.

[0080] Following the block 634, the mobile multi-function device is enabled 636.

In one implementation, the client machine 102 can write certain information into data storage on the mobile multi-function device 104 to inform the mobile multi-function device 104 that the device is now enabled. The mobile multi-function device can then self-determine whether the device is enabled by reading the stored information. Following the block 636 the mobile multi-function device can be disconnected from the client machine.

[0081] In any case, following the block 636, a decision 638 determines whether network setup has been completed. When the decision 638 determines that network setup has been completed, the user can be notified 640 that network setup has completed. The notification can alert the user to perform an action with respect to the mobile multi-function device so that the mobile multi-function device can register with the network and thereafter be utilized thereon. As an example, the notification can be provided to the user by displaying an indication or by sending an electronic message (e.g., email or text message) to the associated client machine. For example, the user can be instructed by the notification to power cycle the mobile multi-function device or connect the mobile multi-function device to the client machine. Following the block 640, the network service setup process 600 ends.

[0082] On the other hand, when the decision 638 determines that the network setup is not complete, the network service setup process 600 can perform other processing 642 unassociated with the network setup. For example, the other processing 642 can pertain to the synchronization of data between the client machine 102 and the mobile multi-function device 104. The other processing 642 can also pertain to media playback at the mobile multi-function device, setting of preferences at the mobile multi-function device or at the client machine, etc. Following the block 642, a decision 644 can deter-

IPR2025-01572
Apple EX1002 Page 864

mine whether completion of the network setup for the mobile multi-function device should be re-checked. In one embodiment, the completion of the network setup can be re-checked periodically (e.g., every 2 minutes). Typically, if the network setup has not properly completed after a number of attempts or period of time, the network service setup process 600 could end and inform the use that the network service was not able to be setup. In any case, when the decision 644 determines that the network setup should be re-checked, the network service setup process 600 can repeat the decision 638 and subsequent blocks to again determine whether network setup has completed. Alternatively, when the decision 644 determines that the network setup should not be re-checked, the network service setup process 600 can repeat the block 642 so that other processing can optionally be performed.

[0083] FIG. 6D is a flow diagram of an alternative portion of the network service setup process 600 according to one embodiment of the invention. In particular, the blocks 646-660 illustrated in FIG. 6D represent an alternative embodiment for the portion of the network service setup process 600 illustrated in FIG. 6C, namely, blocks 636-644. Following the block 634, the mobile multi-function device is enabled 646. In one implementation, the client machine 102 can write certain information into data storage on the mobile multi-function device 104 to inform the mobile multi-function device 104 that the device is now enabled. The mobile multi-function device can then self-determine whether the device is enabled by reading the stored information. In any case, following the block 646, a decision 648 determines whether network setup has been completed. When the decision 648 determines that network setup has been completed, the mobile multi-function device can be instructed 650 to register with the network. The mobile multi-function device can be instructed 650 to register with the network by causing a location update to be issued from the mobile multi-function device. In one implementation, the client machine 102 can send a command to the mobile multi-function device 104 to initiate the location update. In another implementation, the client machine 102 can cause the mobile multi-function device 104 to reset its radio transmitter/receiver (i.e., a portion of its hardware) so as to trigger a location update.

[0084] On the other hand, when the decision 648 determines that the network setup is not complete, a decision 652 determines whether the mobile multi-function device has been disconnected from the client machine. When the decision 652 determines that the mobile multi-function device has not been disconnected, the network service setup process 600 can perform other processing 654 unassociated with the network setup. For example, the other processing 654 can pertain to the synchronization of data between the client machine 102 and the mobile multi-function device 104. The other processing can also pertain to media playback at the mobile multi-function device, setting of preferences at the mobile multi-function device or at the client machine, etc. Following the block 654, the network service setup process 600 returns to repeat the decision 648 to again determine whether network setup has completed.

[0085] Alternatively, when the decision 652 determines that the mobile multi-function device has been disconnected from the client machine, a decision 656 determines whether network setup has completed. When the decision 656 determines that network setup has not completed, other processing 658 can be performed until the network setup has completed. Alternatively, when the decision 656 determines that network setup has completed, the user can be notified 660 that network setup has completed. The notification can alert the user to perform an action with respect to the mobile multi-function device so that the mobile multi-function device can register with the network and thereafter be utilized thereon. As an example, the notification can be provided to the user by displaying an indication or by sending an electronic message (e.g., email or text message) to the user. The electronic message can, for example, be sent to the mobile multi-function device or the associated client machine. For example, the user can be instructed by the notification to power cycle the mobile multi-function device or connect the mobile multi-function device to the client machine. Following the blocks 650 and 660, the network service setup process 600 ends.

[0086] In one embodiment, the mobile multi-function device can store information that can be used to determine whether the mobile multi-function device is enabled. For example, the mobile multi-function device can stored an identifier (e.g., activation identifier) that is provided by a client machine once the mobile multi-function device is to be enabled. In one embodiment, the identifier is stored in a secured manner, such as through use of encryption, digital certificate or other cryptographic technique. The identifier can include or be based on a Subscriber Identity Module (SIM) that is included in the mobile multi-function device while activated. In one implementation, a SIM value, such as a SIM card identifier (e.g., ICCID), read from the SIM card itself within the mobile multi-function device is compared to the identifier stored in a data store (e.g., Flash memory) within the mobile multi-function device. If the identifier matches the read SIM value, then the mobile multi-function device has previously been enabled. As such, the mobile multi-function device can self-determine whether it has been enabled. This enablement verification can, for example, prevent different SIM cards from being used with a mobile multi-function device that has been previously activated while using a different SIM card. An alternative to a SIM is a Universal Subscriber Identity Module (USIM). SIM cards are used with GSM type wireless networks. Other types of networks, such as CMDA, can use other identifiers. Often the identifiers in other networks are not removable from the multi-function device by users. In such cases, the identifier is stored within the device itself such that the identifier is not removable from the device. In such

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 865

cases, the mobile multi-function device can simply store a flag that indicates whether or not the mobile multi-function device is enabled.

[0087] FIG. 7 is a flow diagram of a network service setup process 700 according to one embodiment of the invention. The network service setup process 700 is, for example, processing performed when activating a Mobile Multi-function Device (MMD). For example, the network service setup process 700 can be associated with processing performed when the mobile multi-function device 104 is connected to the client machine 102 illustrated in FIG. 1 so that interaction with the activation server 112 can be performed via the client machine 102 to setup service for the mobile multi-function device 104.

[0088] The network service setup process 700 can begin with a decision 702 that determines whether the mobile multi-function device is attached to the client machine (e.g., personal computer). When the decision 702 determines that the mobile multi-function device is not attached, the network service setup process 700 is not performed. On the other hand, when the decision 702 determines that the mobile multi-function device is attached, the network service setup process 700 can be performed. Once the decision 702 determines that the mobile multi-function device is attached, Mobile Multi-function Device (MMD) information can be read 704 from the multi-function device. In one embodiment, the MMD information can be encrypted so as to prevent unauthorized access. For additional details on preventing unauthorized access to device information, such as the MMD information, see, for example, U.S. Patent Application No. 11/767,447, filed June 22, 2007, and entitled "DEVICE ACTIVATION AND ACCESS," which is hereby incorporated by reference herein. After the MMD information has been read 704, a decision 706 determines whether the mobile multi-function device has already been activated. When the decision 706 determines that the mobile multi-function device has already been activated, then other processing 708 can be performed In other words, in one embodiment, the mobile multi-function device can perform various other processing 708 supported by the device given that the device has been activated. In this regard, the mobile multi-function device can utilize network service. Following the block 708, since the mobile multi-function device has already been activated, the network service setup process 700 can end.

[0089] When the decision 706 determines that the mobile multi-function device has not already been activated, a decision 710 determines that a user activation request has been received. When the decision 710 determines that a user activation request has not been received, the network service setup process 700 awaits a user activation request. Alternatively, when the decision 710 determines that a user activation request has been received, a decision 712 determines whether the user is a new customer. When the decision 712 determines that the user is a new customer, a decision 714 determines whether the customer desires an individual plan or a family plan. When the decision 714 determines that the customer desires an individual plan, processing proceeds to FIGs. 8A-8C where an activation process for an individual plan is described. On the other hand, when the decision 714 determines that the customer desires a family plan, processing proceeds to FIG. 9 where an activation process for a family plan is described.

[0090] On the other hand, when the decision 712 determines that the user is not a new customer, but is instead an existing customer, then a decision 716 determines whether the mobile multi-function device is a new device being substituted for a previously activated device. When the decision 716 determines that the mobile multi-function device is a new device, then processing proceeds to FIG. 10 where an activation process for an existing account is described. Alternatively, when the decision 716 determines that the mobile multi-function device is not new, a decision 718 can determine whether a new line is to be added to an existing account. When the decision 718 determines that a new line is to be added to an existing account, then processing proceeds to FIG. 11 where an activation process for a new line is described. Alternatively, when the decision 718 determines that a new line is not to be provided, then activation can be deemed 720 unavailable. Following the block 720, the network service setup process 700 can end.

[0091] FIGs. 8A-8C are flow diagrams of an activation process 800 according to one embodiment of the invention. The activation process 800 corresponds to activation of a mobile multi-function device with respect to an individual user plan.

[0092] The activation process 800 can begin with a decision 802 that determines whether a phone number is to be transferred. A phone number that can be transferred can be associated with another service provider. Typically, the phone number eligible to be transferred is from another wireless service provider.

However, more generally, the phone number eligible to be transferred can correspond to either a wireless account or a land line account. In any case, when the decision 802 determines that a phone number is to be transferred, an existing phone number and account information for another service provider are provided 804. Typically, the customer will interact with a graphical user interface to provide the information regarding the existing phone number and account information.

[0093] Following the block 804 as well as directly following the decision 802 when a phone number is not to be transferred, customer information can be requested 806. The customer information can include name, address, date of birth, security question(s), e-mail address, account identifier, etc. The customer information can be utilized for one or more accounts that are to be established with one or more service providers. A decision 808 determines whether the customer information has been received. When the decision 808 determines that the customer information has not been received, the activation

IPR2025-01572
Apple EX1002 Page 866

process 800 can await the customer information.

[0094] After the decision 808 determines that the customer information has been received, a decision 810 can determine whether the location of the customer is supported. Here, the service provider typically only supports specific geographical locations. Hence, the customer location can be examined to determine whether it is within a geographical location supported by the system. Hence, when the decision 810 determines that the customer location is not supported by the system of the service provider, the customer can be informed 812 that activation is unavailable. Following the block 812, the activation process 800 can end without activating the mobile multifunction device.

[0095] On the other hand, when the decision 810 determines that the customer location is supported by the system of the service provider, one or more service plans to be offered to the customer can be determined 814. Next, the one or more service plans are offered 816 to the customer. A decision 818 then determines whether the customer has selected one of the service plans. When the decision 818 determines that a service plan has not yet been selected, the activation process 800 can await a plan selection. Alternatively, when the decision 818 determines that a service plan has been selected, billing information can be requested 820. The billing information can be utilized by one or more service providers. A decision 822 determines whether the billing information has been received. When the decision 822 determines that the requested billing information has not been received, the activation process 800 can await the billing information. Once the decision 822 determines that the billing information has been received, account information approval is requested 824. The account information approval can pertain to approval of the customer for the account to be activated. In one example, the account information would be presented to the customer for review and approval. A decision 826 determines whether the account information has been approved. When the decision 826 determines that the account information has not yet been approved, the activation process 800 can await such approval.

[0096] Once the decision 826 determines that the account information has been approved, the activation process 800 requests 828 approval of one or more service agreements. In one example, the one or more service agreements would be presented to the customer for review and acceptance. A decision 830 then determines whether the one or more service agreements had been approved. When the decision 830 determines that the one or more service agreements have not been approved, then the activation process 800 can await such approval. Once the decision 830 determines that the one or more service agreements have been approved, setup of a billing account can be requested 832. A remote server associated with a service provider can receive and process the request to setup a billing account for the customer. The setup of the billing account can utilize the customer information and/or the billing information that has been previously obtained by the activation process 800. Billing accounts can be setup in this manner for one or more service providers.

[0097] Additionally, the activation process 800 can request activation of an account. In other words, the activation being requested 834 can correspond to an account activation process. The account activation can be perform by a remote server, e.g., activation server, associated with a service provider. Following the request 834 for activation of an account, a decision 836 can determines whether the account has been activated. When the decision 836 determines that the account has not yet been activated, a decision 838 can determine whether the account activation has failed. When the decision 838 determines that the account activation has not failed, the activation process 800 can return to repeat the decision 836. Alternatively, when the decision 838 determines that the account information has failed, the customer can be informed 840 of unsuccessful activation. Following the block 840, the activation process 800 ends.

[0098] On the other hand, when the decision 836 determines that the account associated with the customer has been activated, the customer can be informed 842 of the successful activation. Thereafter, the mobile multifunction device can be activated 844. The activation 844 of the mobile multi-function device can, for example, be processing described above with reference to FIGs. 6C or 6D.

[0099] FIG. 9 is a flow diagram of an activation process 900 according to another embodiment of the invention. The activation process 900 is, for example, processing associated with activating a mobile multi-function device for use on a family plan.

[0100] The activation process 900 can begin with a decision 902 that determines whether the mobile multifunction device is to be activated as a family plan. When the decision 902 determines that the mobile multi-function device is not to be activated as a family plan then the mobile multi-function device can alternatively be activated 904 on an individual plan basis. When the decision 902 determines that the mobile multi-function device is to be activated as a family plan, an activation process 906 can be carried out for a family plan. The activation process for a family plan is generally similar to the processing illustrated in FIGs. 8A-8C; however, the account being established is a family account not an individual account and also the service plans normally differ because they pertain to family plans. Following the blocks 904 and 906, the activation process 900 for a family plan is complete.

[0101] FIG. 10 is a flow diagram of an activation process 1000 according to another embodiment of the invention. The activation process 1000 is, for example, processing associated with activation of a new mobile multi-function device by an existing customer of the service provider.

[0102] The activation process 1000 can request 1002

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 867

current account information. Typically, the current account information would be requested 1002 from a customer attempting to activate a mobile multi-function device. A decision 1004 then determines whether the current account information has been received. In one embodiment, the current account information is received from the customer through interaction with a graphical user interface. The current account information is requested so that the customer's current account can be identified. When the decision 1004 determines that the current account information has not been received, the activation process 1000 can await the current account information.

[0103] Once the decision 1004 determines that the current account information has been received, a decision 1006 determines whether the user is authenticated. The authentication of the customer (user) can be achieved in a variety of different ways, including use of a user name, password, and/or a security question, etc. Hence, authenticating the user typically requires user data entry. When the decision 1006 determines that the customer (user) is authorized with respect to the current account, a subscriber status for the current account can be checked 1008. A decision 1010 can then determine whether the account for the subscriber is active. When the decision 1010 determines that the account for the subscriber is active, then processing associated with blocks 814-844 are the activation process 800 illustrated in FIG. 8A-8C can be performed 1012 to activate an account (new or update to existing account) and also activate the mobile multi-function device. On the other hand, when the decision 1006 determines that the user is not authenticated or when the decision 1010 determines that the account is not active, an error indication can be presented 1014. As an example, the error indication can be presented 1014 by a graphical user interface that informs the customer that activation is not available. Following the block 1012 or the block 1014, the activation process 1000 can end.

[0104] FIG. 11 is a flow diagram of an activation process 1100 according to another embodiment of the invention. The activation process 1100 is concerned with adding an additional line to an existing account with a network service provider.

[0105] The activation process 1000 can request 1102 current account information. Typically, the current account information would be requested 1102 from a customer attempting to activate a mobile multi-function device. A decision 1104 determines whether the current account information associated with the customer has been received. In one embodiment, the current account information is received from the customer through interaction with a graphical user interface.

When the decision 1104 determines that the current account information has not been received, the activation process 1100 can await the current account information. Alternatively, when the decision 1104 determines that the current account information has been received, a decision 1106 can determine whether the customer (user) is authorized to access the client account (or its information). When the decision 1106 determines that the customer (user) is authenticated and able to access the account, a subscriber status for the account is checked 1108. A decision 1110 can then determine whether the account associated with the subscriber (customer) is active. When the decision 1110 determines that the account associated with the subscriber is inactive (i.e., not active), an error indication can be presented 1112. In the event that the account associated with the subscriber is inactive, the error indication being presented 1112 can inform the customer that they are unable to add a new line to an existing account because the account is inactive.

[0106] On the other hand, when the decision 1110 determines that the account associated with the subscriber is active, the activation process 1100 can determine 1114 whether an additional line is available to the subscriber. In one embodiment, a subscriber can be allocated up to a determined of number lines for which they may activate. The number of lines available to the subscriber can be determined based on the subscriber's credit history, service plan, anticipated or actual use, etc. When the decision 1116 determines that an additional line is not available to the subscriber, then the subscriber can be informed 1118 that the additional line is not available. In one implementation, such as illustrated in FIG. 11, when an additional line can still be available if the subscriber provides a deposit (e.g., security deposit), the subscriber can be so informed 1118. Alternatively, when the decision 1116 determines that the additional line is available, the activation process 1100 can perform various previously described operations to activate the mobile multi-function device at block 1120. In one embodiment, the activation operations are associated with blocks 802, 804 and 810-844 of the activation process 800 illustrated in FIGs. 8A-8C. Following the blocks 1112, 1118 and 1120, the activation process 1100 can end.

[0107] Another aspect of the invention pertains to online provisioning methods and graphical user interfaces therefore. The provisioning methods enable an end user to activate a mobile communication device (e.g., mobile phone). In one embodiment, an end user can connect a mobile communication device to a computing device, such as a personal computer, and then perform an online activation process with a wireless service provider. The invention can provide automation and flexibility to activation of wireless communication devices.

[0108] FIGs. 12A-12C are flow diagrams of a mobile device provisioning process 1200 according to one embodiment of the invention. The mobile device provisioning process 1200 is, for example, performed by a server, such as the activation server 112 of the activation system 100 illustrated in FIG. 1.

[0109] The mobile device provisioning process 1200 can begin with a decision 1202. The decision 1202 can determine whether a new mobile device needs to be provisioned (or activated). The new mobile device, for ex-

IPR2025-01572
Apple EX1002 Page 868

ample, can refer to a mobile device that requires provisioning in order to utilize a wireless network for voice (and/or data) communications. The new mobile device can, for example, be recognized by a client machine, such as the client machine 102 illustrated in FIG. 1, when the mobile device connects with the client machine. The client machine can then in turn interact with the activation server to present suitable graphical user interfaces that assist the user of the mobile device in provisioning (or activating) the mobile device. Hence, when the decision 1202 determines that a new mobile device is not present, then the mobile device provisioning process 1200 awaits the presence of a new mobile device. In other words, until a new mobile device is present, the mobile device provisioning process 1200 simply waits to recognize a new mobile device. On the other hand, once the decision 1202 determines that a new mobile device has been recognized, an initial registration page is displayed 1204. The initial registration page can provide initial information to a user regarding registration of a mobile device.

[0110] FIG. 13 is a screen shot of an exemplary initial registration page 1300 according to one embodiment of the invention. The initial registration page 1300 illustrated in FIG. 13 provides initial registration information regarding a device entitled "Debbie's iPhone" which in this example pertains to a mobile phone. In one embodiment, the mobile phone is a multi-function device. After the initial registration page is displayed 1204, a decision 1206 can determine whether a user continues with the mobile device provisioning process 1200. When the decision 1206 determines that the user has not yet elected to continue, the mobile device provisioning process 1200 can await such a request. Alternatively, the user could instead request to cancel the mobile device provisioning process 1200, in which case the mobile device provisioning process 1200 could end.

[0111] On the other hand, when the decision 1206 determines that the user has requested to continue with the mobile device provisioning process 1200, a customer status page can be displayed 1208. In general, the customer status page can allow a customer (user) to specify whether or not they are an existing customer to the wireless network provider, in this example, AT&T Wireless. Additionally, the customer status page may enable the customer to specify whether they are activating on an individual plan or a group plan, or whether they wish to keep their current phone number (i.e., transferring the phone number) or create a new phone number.

[0112] FIG. 14 is a screen shot of an exemplary customer status page 1400 according to one embodiment of the invention. The customer status page 1400 allows a new wireless network service customer to activate a new phone on an individual plan. Here, the customer may or may not desire to transfer their current mobile phone number. Further, the customer status page 1400 can allow an existing wireless network service customer to either keep their current phone number or create a new phone number for the particular mobile device being provisioned.

[0113] After the customer status page is displayed 1208, a decision 1210 determines whether the customer is a new customer. As an example, this determination can be made following submission of the customer status page 1400 which enables the user to indicate whether or not they are an existing customer.

[0114] Although not illustrated in FIGs. 12A-12C, the mobile device provisioning process 1200 can further display a number transfer page. The number transfer page can assist a user in transferring an existing number from another service provider to be used with the particular mobile device being provisioned.

[0115] FIG. 15 is a screen shot of an exemplary screen shot of a mobile number transfer page 1500. The mobile number transfer page 1500 includes a data entry region 1502 that enables a user to provide existing account information in the case where an existing mobile number is to be transferred. FIG. 16 is a screen shot of an exemplary screen shot of a landline number transfer page 1600. The landline number transfer page 1600 includes a data entry region 1602 that enables a user to provide existing account information in the case where an existing landline number is to be transferred.

[0116] When the decision 1210 determines that the user is a new customer, a service plan selection page can be displayed 1212. In general, the service plan selection page provides one or more available service plans to the customer. A customer can then select one of the available service plans.

[0117] FIG. 17A and 17B are screen shots of an exemplary service plan selection page 1700 according to one embodiment of the invention. The service plan selection page 1000 allows the customer to select from one of six service plans 1702-1712, each of which can offer a different package of services at different rates. A first three of the service plans are illustrated in FIG. 17A, and a second three of the service plans are illustrated in FIG. 17B.

[0118] Following the display 1212 of the service plan selection page, a decision 1214 can determine whether a service plan has been selected. When the decision 1214 determines that a service plan has not yet been selected, the mobile device provisioning process 1200 can await such a selection. On the other hand, once the decision 1214 determines that a service plan has been selected, as well as following the decision 1210 when the customer is not a new customer, a customer account page can be displayed 1216. The customer account page can allow an existing customer to login to their account. The account is, for example, associated with an on-line media store, such as the iTunes® media store.

[0119] FIG. 18 is a screen shot of an exemplary customer account page 1100 according to one embodiment of the invention. The customer account page 1100 includes a sign-in section 1802 that allows an existing account holder to sign-in, with an identifier (e.g., Apple ID) and password.

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 869

[0120] After the customer account page has been displayed 1216, a decision 1218 can determine whether the customer is an existing account holder. When the decision 1218 determines that the customer has an existing account, the customer can login 1220 to the account. Alternatively, when the decision 1218 determines that the customer does not have an existing account, or following the block 1220 after a successful login to an account, a customer information entry page is displayed 1222. The customer information entry page can facilitate a user in entering customer information that is to be utilized by either the wireless network service provider or the media asset provider (e.g., on-line media store). For a customer with an existing account, the customer information can be pre-entered and/or the certain subsequent portions of the remaining processing for the mobile device provisioning process 1200 could be simplified or eliminated. For a customer without an existing account with the on-line media store, the customer information entry page can also allow the customer to create a new account with the on-line media store.

[0121] FIG. 19 is a screen shot of a customer information entry page 1900 according to one embodiment of the invention. The customer information entry page 1900 allows entry of basic customer information to be utilized in creating one or more accounts. The customer information can, for example, include information pertaining to the customer, such as e-mail address, password, security question and answer, and date of birth.

[0122] Once the customer has entered the requested customer information, the mobile device provisioning process 1200 can continue. A decision 1224 determines whether customer information has been received. When the decision 1224 determines that the customer information has been received, such as by completion of the customer information entry page, a billing information page can be displayed 1226. The billing information page enables a customer to provide billing information to be utilized to pay for the service plan that was previously selected by the customer. The billing information can also be used by another service provider, such as an online media store. It should be noted that sharing of customer information and/or billing information between two or more service providers provides an efficient and user friendly system is provided.

[0123] FIG. 20 illustrates an exemplary billing information page 2000 according to one embodiment of the invention. The billing information page 2000 provides a means for the customer to enter various billing information, such as name, billing address, phone number, social security number, credit card number, security code, and expiration date. The billing information can be used by one or more service providers, in this example, AT&T Wireless as the wireless service provider and iTunes® media store as an online media service provider.

[0124] After the billing information page is displayed 1226, a decision 1228 determines whether billing information has been received. When the decision 1228 determines that billing information has not been received, then the mobile device provisioning process 1200 awaits such billing information. On the other hand, when the decision 1228 determines that billing information has been received, a terms and condition page can be displayed 1230. The terms and conditions page can provide the customer with the terms and conditions of the one or more legal agreements that are being established with the customer.

[0125] FIG. 21A is an exemplary screen shot of a first terms and conditions page 2100 according to one embodiment of the invention. In this example, the customer is required to read and agree to a software license/usage agreement 2102 with respect to Apple Computer, Inc. for use of the iTunes® media store. FIG. 21B is an exemplary screen shot of a second terms and conditions page 2150 according to one embodiment of the invention. In this example, the customer is required to read and agree to a wireless service agreement 2502 with a wireless service provider. The terms and conditions pages 2100 and 2150 require that the user accept the respective terms and conditions of these agreements in order to continue.

[0126] Following the display 1230 of the terms and conditions page, a decision 1232 determines whether the customer has accepted the various terms and conditions. When the decision 1232 determines that the customer has not accepted the terms and conditions, then the mobile device provisioning process 1200 awaits such acceptance. Once the decision 1232 determines that the customer has accepted the various terms and conditions, a review information page can be displayed 1234. The review information page allows a user to finally review the information regarding the service plan (i.e., wireless network service) being established for the mobile device for the customer information, and the associated billing information.

[0127] FIG. 22 is a screen shot of an exemplary review information page 2200 according to one embodiment of the invention. The review information page 2200 summarizes the billing and plan information concerning the mobile device being activated. For example, as shown in FIG. 22, the review information page 2200 can specify the billing amount and the manner in which the customer is to be billed, a service plan and a brief description thereof, additional fees and explanation of additional costs.

[0128] After the review information page has been displayed, a decision 1236 can determine whether the mobile device provisioning process 1200 should continue. When the decision 1236 determines that the customer has decided to continue the mobile device provisioning process 1200, one or more setup completion pages can be displayed 1238. The one or more setup completion pages can inform the customer that the setup (or activation) of their mobile device is processing and/or has successfully completed. The setup completion page may also provide a phone number for the mobile device to the customer or indicate that the existing phone number is being transferred. The setup completion page may also

EPODOC(ID: <EP 1942698A1 | >

IPR2025-01572
Apple EX1002 Page 870

permit the customer to provide a name for the mobile device.

[0129] FIG. 23 is an exemplary screen shot of a setup completion page 2300 according to one embodiment of the invention. The setup completion page 2300 informs the customer that activation of the mobile device is being processed. FIG. 24A is an exemplary screen shot of a setup completion page 2400 according to another embodiment of the invention. The setup completion page 2400 provides the customer with a phone number 2402. FIG. 24B is an exemplary screen shot of a setup completion page 2450 according to still another embodiment of the invention. The setup completion page 2450 informs the customer that transfer of the existing phone number is ongoing. In one embodiment, the setup completion page 2400 and the setup completion page 2450 are alternative pages that are chosen dependent on whether a new phone number is being assigned or whether an existing phone number is being transferred.

[0130] After the setup completion page has been displayed 1238, a decision 1240 determines whether the customer desires to continue on with the mobile device provisioning process 1200. When the decision 1240 determines that the customer has not yet decided to continue, the mobile device provisioning process 1200 awaits the request to continue. Once the decision 1240 determines that the customer has requested to continue, a device preference page is displayed 1242. The device preference page can, for example, be provided by a media management application. In this regard, the media management application can assist the customer with the setting of one or more preferences concerning the mobile device that has just been provisioned (or activated). Alternatively, the customer can choose not to continue to the device preference page and instead end the mobile device provisioning process 1200. In any case, following the block 1242 (or alternatively following the block 1238), the mobile device provisioning process 1200 can end as the provisioning of the mobile device has been initiated and perhaps completed. Following the mobile device provisioning process 1200, the mobile device can thereafter be controlled or managed by the media management application. To the extent that the customer has set one or more preferences concerning the mobile device, the media management application can thereafter operate in accordance with the one or more preferences when interacting with or on behalf of the mobile device.

[0131] FIG. 25 is an exemplary screen shot of a device preference page 2500 according to one embodiment of the invention. The device preference page 2500 includes a source region 2501 and a preference information region 2502. A visual selector 2503 indicates selection of a device referred to as "Debbie's iPhone". For this selected device, the preference information area 2502 displays information 2506 regarding preferences associated with the particular device. In this specific example, a summary tab 2504 is active so that a summary preference window is displayed in the preference information area 2502. The summary preference window includes information describing the particular device, such as name, size, software version and serial number. The summary preference window also provides version information 2508 indicating whether or not an updated version of any software components might be available. Further, the summary preference window includes an options section 2510 that allows a customer to select one or more predetermined options regarding the mobile device. Device preferences can be set by a user for a plurality of different types of media. The device preferences can also be set differently for different types of media. The device preference page 2500 includes other tabs for distinct media types, including music, movies, TV shows, podcasts, photos, personal and games. These device preferences can be synchronization preferences used when synchronizing the media device with the client machine. For additional information on synchronization and synchronization preferences see (i) U.S. Provisional Patent Application No. 60/879,319, filed January 7, 2007, and entitled "MULTI-DEVICE DATA SYNCHRONIZATION OR BACKUP VIA A HOST DEVICE," which is hereby incorporated herein by reference; and (ii) U.S. Patent Application No. 11/679,082, filed February 26, 2007, and entitled "DATA SYNCHRONIZATION WITH HOST DEVICE IN ACCORDANCE WITH SYNCHRONIZATION PREFERENCES," which is hereby incorporated herein by reference.

[0132] As noted above, the provisioning method can also be used by existing customers. For example, an existing customer may get a new wireless communication device (e.g., mobile phone, multi-function device, etc.) that they want to use in place of their current wireless communication device. In one embodiment, the service plan (or rate plan) offered to the end user can have a predetermined minimum term (e.g., 2 years) or cancellation penalty duration. In one implementation, the user's new service plan will reset such minimum period(s) regardless of whether the user has already exceed the minimum period(s) for the user's existing plan.

[0133] FIG. 26 is a screen shot of an exemplary customer status page 2600 according to one embodiment of the invention. The customer status page 2600 allows a new wireless network service customer to activate a new mobile phone (i.e., mobile device) on pre-existing account in place of an existing mobile phone, whereby the phone number for the new mobile phone is the same as the phone number previously used for the existing mobile phone. Since the customer is an existing customer, an account information page can also be displayed. The account information page can permit the user to enter account information concerning their account with the wireless service provider. The account information serves to identify the pre-existing account of the user. As such, an activation server can locate the user account and associate the new mobile phone with the pre-existing account. FIG. 27 is a screen shot of an exemplary ac-

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 871

count information page 2700 according to one embodiment of the invention. The account information page 2700 includes an account information entry area 2702 allows a user to enter account information.

[0134] An existing customer can also use the computer-assisted provisioning process to add an additional line to an existing account. FIG. 28 is a screen shot of an exemplary customer status page 2800 according to one embodiment of the invention. The customer status page 2800 allows an existing wireless network service customer to activate a new mobile phone on pre-existing account. Since the customer is an existing customer, an account information page can also be displayed. The account information page can permit the user to enter account information concerning their account with the wireless service provider. The account information serves to identify the pre-existing account of the user. As such, an activation server can locate the user account and associate the new mobile phone with the pre-existing account. FIG. 29 is a screen shot of an exemplary account information page 2900 according to one embodiment of the invention. The account information page 2900 includes an account information entry area 2902 allows a user to enter account information. Still further, in this scenario the pre-existing account is assumed to be an individual account. Hence, in one embodiment, an account type selection page can be displayed. FIG. 30 is a screen shot of an exemplary account type selection page 3000 according to one embodiment of the invention. The account type selection page 3000 allows the customer to choose to activate the new mobile phone on an individual plan or to instead convert to a family plan. Typically, with a family plan, the various mobile phones within the group can share service time (e.g., share plan minutes).

[0135] A new customer can also use the computer-assisted provisioning process to activate multiple mobile devices. FIG. 31 is a screen shot of an exemplary customer status page 3100 according to one embodiment of the invention. The customer status page 3100 allows a new customer for wireless network service to activate one mobile phone or multiple mobile phones. In one embodiment, when two or more mobile phones are to be activated an account type selection page can be displayed to enable the customer to choose between individual plans or family plans. FIG. 32 is a screen shot of an exemplary account type selection page 3200 according to one embodiment of the invention. The account type selection page 3200 allows the customer to choose to activate each of the multiple new mobile phones on individual plans or to instead activate all of the multiple new mobile phones on a family plan. Typically, with a family plan, the various mobile phones within the group can share service time (e.g., share plan minutes). In this example, the conversion to a family plan requires calling customer support; however, in other embodiments such can be part of the computer-assisted provisioning.

[0136] Mobile device provisioning can also enable remote provisioning of multiple wireless communication devices. For example, wireless service providers often refer to multiple devices on a primary account as a "family plan". Activation of multiple devices for such a primary account can require additional operations. In one embodiment, a first mobile device is connected to the host computer, such as using a USB connection, and then for the subsequent one or more mobile device to be also activated for the primary account can be identified to the provisioning server by having an end-user manually enter an identifier that is provided with another mobile device. For example, the identifier can be provided on or within a package containing the another mobile device. Hence, in would be possible for an end-user to activate a mobile device without it being present.

[0137] In one embodiment, the activation process uses two identifiers, IMEI and ICCID, when activating a mobile device. However, neither of these identifiers have built-in error correct or validation. Hence, manual entry of these identifiers by end-users could lead to failed or improper activation. One embodiment to enhance activation in such situations is to provide end-users with a computed identifier that uniquely maps to the needed IMEI and ICCID identifiers. The computed identifier can be more compact (i.e., less digits) and thus easier for manual entry. Moreover, the computed identifier can include error correction to guard against improper entry of the computed identifier.

[0138] Mobile device provisioning can also restrict payment options to those consumers that have low credit scores. For example, a wireless service provider may not desire to activate a wireless service plan to those customers that have poor credit. Hence, in one embodiment, the wireless service provider can offer different payment options to different customers dependent on at least credit information (e.g., credit score). For example, customers with poor credit can be required to pay a deposit or to pre-pay for such service.

[0139] In some cases, a new customer can be limited to service plans that require prepayment. In one embodiment, the provisioning process can decide whether prepayment is required based on the credit history of the customer. The credit history can, for example, result from a credit report on the customer. FIG. 33 is a screen shot of an exemplary prepayment requirement page 3300. The exemplary prepayment requirement page 3300 can present the customer with one or more option on activating wireless service. The exemplary prepayment requirement page 3300 allows the customer to (i) provide a pre-approval credit check code and continue activation, (ii) agree to a prepaid plan (e.g., with advance monthly payment via credit or debit card) and continue activation, or (iii) restart/cancel the activation process.

[0140] As noted above, the provisioning method can also be used by existing customers. For example, an existing customer may get a new wireless communication device (e.g., mobile phone, multi-function device, etc.) that they want to use it in place of their current wireless communication device. In one embodiment, the

EPODOC: EP 1942698A1 1 >

IPR2025-01572
Apple EX1002 Page 872

service plan offered to the end user can have a predetermined minimum term (e.g., 2 years) or cancellation penalty duration. In one implementation, the user's new service plan will reset such minimum period regardless of whether the user has already exceed the minimum period for the user's existing plan.

[0141] FIG. 34 is a block diagram of a mobile multi-function device 3400 according to one embodiment of the invention. The mobile multi-function device 3400 can include the circuitry of the mobile multi-function device 104 illustrated in FIG. 1 and/or can perform the operations described with reference to FIGs. 3 and 4. The mobile multi-function device 3400 includes hardware and software components to provide at least two functions, namely, a media playback function and a wireless voice communications function. When providing media playback, the mobile multi-function device 3400 can operate as a media player capable of playing (including displaying) media items. The media items can, for example, pertain to audio items (e.g., audio files or songs), videos (e.g., movies) or images (e.g., photos). When providing wireless voice communications, the mobile multi-function device 3400 can operate a mobile telephone (e.g., cellular phone).

[0142] The mobile multi-function device 3400 includes a processor 3402 that pertains to a microprocessor or controller for controlling the overall operation of the mobile multi-function device 3400. The mobile multi-function device 3400 stores media data pertaining to media items in a file system 3404 and a cache 3406. In one embodiment, the file system 3404 is implemented by a storage disk or a plurality of disks. In another embodiment, the file system 3404 is implemented by EEPROM or Flash type memory. The file system 3404 typically provides high capacity storage capability for the mobile multi-function device 3400. However, since the access time to the file system 3404 is relatively slow, the mobile multi-function device 3400 can also include a cache 3406. The cache 3406 is, for example, Random-Access Memory (RAM) provided by semiconductor memory. The relative access time to the cache 3406 is substantially shorter than for the file system 3404. However, the cache 3406 does not have the large storage capacity of the file system 3404. Further, the file system 3404, when active, consumes more power than does the cache 3406. The power consumption is often a concern when the mobile multi-function device 3400 is a portable mobile multi-function device that is powered by a battery 3424. The mobile multi-function device 3400 also includes a RAM 3420 and a Read-Only Memory (ROM) 3422. The ROM 3422 can store programs, utilities or processes to be executed in a non-volatile manner. The ROM 3422 can be implemented by an EEPROM or Flash type memory so as to provide writable non-volatile data storage. The RAM 3420 provides volatile data storage, such as for the cache 3406.

[0143] In one embodiment, to support wireless voice communications, the mobile multi-function device 3400 includes a transceiver 3426 and a SIM card 3428. The transceiver 3426 supports wireless communication with a wireless network (such as a wireless cellular network). The SIM card 3428 includes an identifier (e.g., SIM identifier) can be used by the mobile multi-function device 3400 to gain access and utilize the wireless network. In other embodiments, a SIM card 3428 is not utilized.

[0144] The mobile multi-function device 3400 also includes a user input device 3408 that allows a user of the mobile multi-function device 3400 to interact with the mobile multi-function device 3400. For example, the user input device 3408 can take a variety of forms, such as a button, keypad, dial, etc. Still further, the mobile multi-function device 3400 includes a display 3410 (screen display) that can be controlled by the processor 3402 to display information to the user. A data bus 3411 can facilitate data transfer between at least the file system 3404, the cache 3406, the processor 3402, and the CODEC 3412.

[0145] In one embodiment, the mobile multi-function device 3400 serves to store a plurality of media items (e.g., songs) in the file system 3404. When a user desires to have the mobile multi-function device play a particular media item, a list of available media items is displayed on the display 3410. Then, using the user input device 3408, a user can select one of the available media items. The processor 3402, upon receiving a selection of a particular media item, supplies the media data (e.g., audio file) for the particular media item to a coder/decoder (CODEC) 3412. The CODEC 3412 then produces analog output signals for a speaker 3414. The speaker 3414 can be a speaker internal to the mobile multi-function device 3400 or external to the mobile multi-function device 3400. For example, headphones or earphones that connect to the mobile multi-function device 3400 would be considered an external speaker.

[0146] The mobile multi-function device 3400 also includes a bus interface 3416 that couples to a data link 3418. The data link 3418 allows the mobile multi-function device 3400 to couple to a host device (e.g., host computer or power source). The data link 3418 can also provide power to the mobile multi-function device 3400.

[0147] The various aspects, embodiments, implementations or features of the invention can be used separately or in any combination.

[0148] The invention can be implemented by software, hardware or a combination of hardware and software. The invention can also be embodied as computer readable code on a computer readable medium. The computer readable medium is any data storage device that can store data which can thereafter be read by a computing device (e.g., computer system). Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves. The computer readable medium can also be distributed over network-coupled computer systems so that the computer readable code is stored and executed in a distributed

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 873

fashion.

[0149] The advantages of the invention are numerous. Different aspects, embodiments or implementations may, but need not, yield one or more of the following advantages. One advantage of the invention is that mobile devices can be setup or activated to operate on wireless networks by end users. Another advantage of the invention is that setup or activation can be substantially automated and controlled by a computer-implemented system to facilitate setup or activation with a service provider (e.g., wireless service provider). Another advantage of the invention is that graphical user interfaces can be presented to users so as to enable end users to easily activate mobile devices. Still another advantage of the invention is that more than one account for different service providers can be concurrently arranged in an efficient and user friendly manner. Yet still another advantage of the invention is that mobile devices can be largely disabled until properly activated with a service provider.

[0150] The many features and advantages of the present invention are apparent from the written description. Further, since numerous modifications and changes will readily occur to those skilled in the art, the invention should not be limited to the exact construction and operation as illustrated and described. Hence, all suitable modifications and equivalents may be resorted to as falling within the scope of the invention.

Claims

1. A computer-implemented method for activating wireless network service for an electronic device through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said method comprising:

   receiving device information from the electronic device when the electronic device is attached to the host device;
   acquiring customer information pertaining to the customer;
   receiving a service plan selection from the customer;
   receiving billing information for payment of the service plan; and
   initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider, wherein the wireless service account being activated is based on the customer information, the service plan and the billing information.

2. A computer-implemented method as recited 1, wherein said method further comprises:

   enabling, following said activating, the electronic device for usage of at least one operation that was previously restricted prior to said enabling.

3. A computer-implemented method as recited 1, wherein said method further comprises:

   obtaining a credit indication for the customer; and
   determining one or more service plans that are made available to the customer based at least in part on the credit indication for the customer,

   wherein the service plan selection is one of the one or more service plans.

4. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   requiring formation of a media account with the online media store when the customer does not already have a media account with the online media store.

5. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   thereafter initiating activation of the wireless network service for the electronic device associated with the customer.

6. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   presenting account information for approval; and
   receiving approval from the customer for the account information.

7. A computer-implemented method as recited in claim 1, wherein said method further comprises:

   presenting at least one service agreement for approval; and
   receiving approval of the at least one service agreement.

8. A computer-implemented method as recited in any of claims 1-7, wherein the host device is a personal computer, and wherein said method is performed by an application program operating on the personal computer.

9. A computer-implemented method as recited in claim 8, wherein the application program is a media management application.

10. A computer-implemented method for activating an

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 874

electronic device for wireless network service through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said method comprising:

receiving device information from the electronic device while the electronic device is attached to the host device;
acquiring customer information pertaining to the customer;
offering the user one or more service plans;
receiving a user selection of one of the service plans; and
receiving billing information for payment of the selected service plan.

11. A computer-implemented method as recited in claim 10, wherein said method further comprises:

offering the user a plurality of payment options; and
receiving a user selection of one of the payment options.

12. A computer-implemented method as recited in claim 10, wherein said method further comprises:

initiating activation of an account for the customer whereby the electronic device is provided with access to wireless network service in accordance with the selected service plan.

13. A computer-implemented method as recited in claim 10, wherein said method further comprises:

activating the electronic device for use with the wireless network service in accordance with the selected service plan.

14. A computer-implemented method as recited in claim 10, wherein said activating comprises:

enabling the electronic device; and
initiating setup of the wireless network service to permit usage by the electronic device.

15. A computer-implemented method as recited in claim 10, wherein the user is an end user and wherein the user selections are made by the user by a computer program operating on the host device.

16. A computer-implemented method as recited in claim 10, wherein said method is performed by an activation server that is operatively connected to the host device via a network.

17. A computer-implemented method as recited in claim 10, wherein said method is performed by the host device.

18. A computer-implemented method as recited in claim 10, wherein said method further comprises:

establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

19. A computer-implemented method as recited in claim 18, wherein said method further comprises:

thereafter activating the wireless network service for the electronic device associated with the user.

20. A computer-implemented method as recited in claim 10, wherein the electronic device is a multi-function device.

21. A computer-implemented method as recited in claim 10, wherein the electronic device comprises a mobile phone.

22. A computer-implemented method as recited in claim 10-21, wherein said method further comprises:

determining whether the user has a media account with an online media store.

23. A computer-implemented method as recited in claim 22, wherein said method further comprises:

requiring formation of a media account with the online media store when said determining determines that the user does not have a media account with the online media store.

24. A computer-implemented method as recited in claim 23, wherein said method further comprises:

establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

25. A computer-implemented method as recited in claim 24, wherein said method further comprises:

thereafter activating the wireless network service for the electronic device associated with the user.

26. A computer-implemented method as recited in claim 25, wherein said offering of one or more payment options is dependent on the credit worthiness of the

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 875

user.

27. A computer-implemented method for activating an electronic device for wireless network service from a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said method comprising:

receiving device information from the electronic device when the electronic device is attached to the host device;
determining whether the electronic device has already been activated based on the device information; and
automatically initiating activation of the electronic device when said determining determines that the electronic device has not already been activated.

28. A computer-implemented method as recited in claim 27, wherein the host device is a personal computer, and wherein said method is performed by an application program operating on the personal computer.

29. A computer-implemented method as recited in claim 28, wherein the electronic device is a multi-function device, and wherein one function of the multi-function device is a wireless phone function, and another function of the multi-function device is a media playback function.

30. A computer-implemented method as recited in claim 29, wherein the application program is a media management application.

31. A computer readable medium including at least computer executable program code tangibly embodied therein for activating wireless network service for an electronic device through use of a client computing device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said computer readable medium comprising:

computer program code for receiving device information from the electronic device;
computer program code for acquiring customer information pertaining to the customer;
computer program code for receiving a service plan selection from the customer;
computer program code for receiving billing information for payment of the service plan; and
computer program code for initiating activation of a wireless service account for use of the electronic device with the wireless network service provided by the wireless network service provider.

32. A computer readable medium as recited in claim 31, wherein said computer readable medium further comprises:

computer program code for detecting connection of the electronic device to the host device; and

wherein said computer program code for receiving device information receives, the device information from the electronic device without user interaction once the electronic device is connected to the host device.

33. A computer readable medium including at least computer executable program code tangibly embodied therein for activating an electronic device for wireless network service through use of a host device, the electronic device being associated with a customer for wireless network service provided by a wireless network service provider, said computer readable medium comprising:

computer program code for receiving device information from the electronic device while the electronic device is attached to the host device;
computer program code for acquiring customer information pertaining to the customer;
computer program code for offering the user one or more service plans;
computer program code for receiving a user selection of one of the service plans; and

computer program code for receiving billing information for payment of the selected service plan.

34. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

computer program code for offering the user a plurality of payment options; and
computer program code for receiving a user selection of one of the payment options.

35. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

computer program code for initiating activation of an account for the customer whereby the electronic device is provided with access to wireless network service in accordance with the selected service plan.

36. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

IPR2025-01572
Apple EX1002 Page 876

computer program code for activating the electronic device for use with the wireless network service in accordance with the selected service plan.

37. A computer readable medium as recited in claim 33, wherein said computer program code for activating comprises:

computer program code for enabling the electronic device; and
computer program code for initiating setup of the wireless network service to permit usage by the electronic device.

38. A computer readable medium as recited in claim 33, wherein the user is an end user and wherein the user selections are made by the user by a computer program operating on the host device.

39. A computer readable medium as recited in claim 33, wherein said computer readable medium further comprises:

computer program code for establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

40. A computer readable medium as recited in claim 39, wherein said computer readable medium further comprises:

computer program code for thereafter activating the wireless network service for the electronic device associated with the user.

41. A computer-implemented method as recited in claim 33, wherein the electronic device is a multi-function device.

42. A computer-implemented method as recited in claim 33, wherein the electronic device comprises a mobile phone.

43. A computer-implemented computer readable medium as recited in any of claims 23-42, wherein said computer readable medium further comprises:

computer program code for determining whether the user has a media account with an online media store.

44. A computer readable medium as recited in claim 43, wherein said computer readable medium further comprises:

computer program code for requiring formation of a media account with the online media store when said determining determines that the user does not have a media account with the online media store.

45. A computer readable medium as recited in claim 44, wherein said computer readable medium further comprises:

computer program code for establishing wireless service account for the user, the wireless service account pertaining to the selected service plan and being paid for in accordance with the billing information.

46. A computer readable medium as recited in claim 45, wherein said computer readable medium further comprises:

computer program code for activating the wireless network service for the electronic device associated with the user.

47. A computer readable medium as recited in claim 46, wherein said computer program code for offering of one or more payment options is dependent on the credit worthiness of the user.

48. A graphical user interface to assist an end user in activating an account for an electronic device having wireless communication capabilities, the account being with respect to a wireless service provider providing wireless network service, said graphical user interface comprising:

a plurality of display screens that are presented on a display device associated with a host computer, said display screens includes at least:

an end user status page to facilitate selection of a type of activation;
a service plan selection page to facilitate selection of a service plan for the wireless network service;
a media account page for a media account associated with an online media store so that a user can create a new media account or login to an existing media account;
an end user information entry page to facilitate entry of end user information;
a billing information page to facilitate entry of billing information for one or both the user media account and a wireless account;
a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider; and
an activation page to inform the end user of

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 877

activation information.

49. A graphical user interface as recited in claim 48, wherein said display screens further comprises:

a final review and submit page to initiate activation of the account for the electronic device with respect to the wireless service provider.

50. A graphical user interface as recited in claim 48, wherein the final review and submit page can further initiate creation of the new media account for the user not having the existing media account.

51. A graphical user interface as recited in claim 48, wherein said plurality of display screens further comprises:

a device preference page to assist the end user with setting one or more preferences or options to be applied to the operation of the electronic device.

52. A graphical user interface as recited in claim 48, wherein the end user status page enables a user to select from a plurality of types of activation.

53. A graphical user interface as recited in claim 52, wherein the types of activation include an individual plan and a family plan.

54. A graphical user interface as recited in claim 52, wherein the types of activation include a new individual plan, an existing individual plan, a new family plan, and an existing family plan.

55. A graphical user interface as recited in claim 48, wherein the electronic device is a multi-function device, and wherein the multi-function device supports at least wireless voice communication and media playback.

56. A graphical user interface as recited in claim 48, wherein said plurality of display screens further comprises:

a media account page for identifying a media account for the end user.

57. A graphical user interface as recited in claim 48, wherein the type of activation pertains to individual plan activation or family plan activation.

58. A graphical user interface as recited in claim 48, wherein one of the types of activation pertains to use of an existing phone number or a new phone number.

59. A graphical user interface as recited in claim 48, wherein said service plan selection page presents information on a plurality of service plans and their costs and enables the end user to select from the service plans.

60. A graphical user interface as recited in claim 48, wherein the billing information provided via said billing information page includes information pertaining to name and billing address for the end user and credit card number.

61. A graphical user interface as recited in claim 48, wherein the activation completion page informs the end user of a phone number associated with the electronic device being activated.

62. A graphical user interface as recited in claim 48, wherein said plurality of display screens further comprises:

a device preference page to assist the customer with setting one or more preferences or options to be applied to the operation of the electronic device.

63. A graphical user interface as recited in claim 48, wherein said graphical user interface comprises:

a transfer number page for identifying a phone number and an existing account, wherein the phone number to be transferred is to be used with the account being activated and associated with the electronic device.

64. A graphical user interface as recited in claim 48, wherein said graphical user interface is presented on a display device associated with a computing device, and wherein the electronic device is electrically coupled to the computing device.

65. A graphical user interface as recited in claim 64, wherein the electronic device is a multi-function device, and wherein one function of the multi-function device is a wireless phone function, and another function of the multi-function device is a media playback function.

66. A graphical user interface as recited in claim 65, wherein the application program is a media management application.

67. A computer-implemented method for activating an electronic device for wireless network service, the electronic device being associated with a customer of a wireless service provider associated with the wireless network service, said method comprising:

informing an activation server of an electronic

IPR2025-01572
Apple EX1002 Page 878

device having wireless communication device that is to be activated for wireless network service;
displaying a customer status page to facilitate selection of a type of activation;
specifying to the activation server a type of activation desired by the customer;
displaying a service plan selection page to facilitate selection of a service plan for the wireless network service;
informing the activation server of a selected service plan;
displaying a customer account page to facilitate login to or creation of a user media account with an online media store;
providing account information for the user media account for the customer;
displaying a customer information entry page;
providing customer information to the activation server;
displaying a billing information page to facilitate entry of billing information for one or both the user media account and a wireless account;
informing the activation server of the billing information;
displaying a terms and conditions page regarding legal agreements with the online media store and with the wireless service provider;
informing the activation server of acceptance of the legal agreements;
displaying an information review page;
informing the activation server of approval of the information provided on the information review page;
displaying an activation completion page; and
displaying a device preference page to assist the customer with setting one or more preferences or options to be applied to the operation of the electronic device.

68. A method as recited in claim 67, wherein said displaying by said method is on a display device associated with a client computing device having the electronic device operatively coupled thereto.

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 879

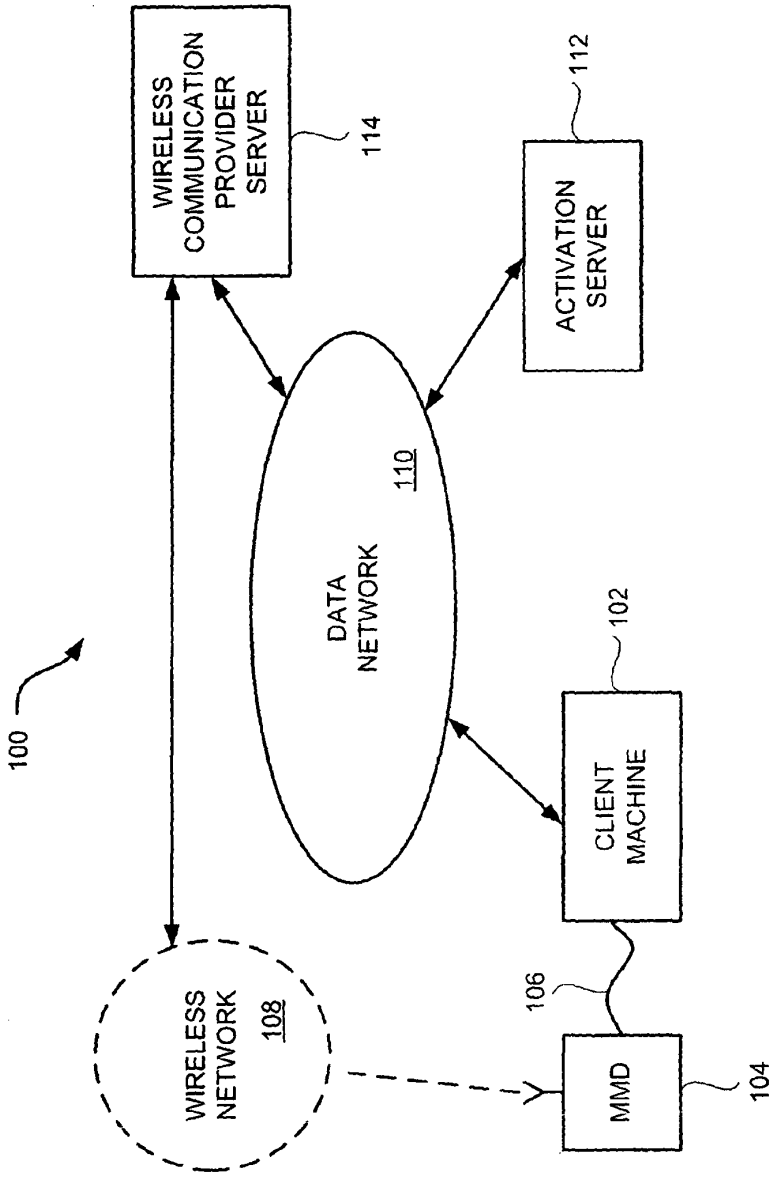


FIG. 1

EPNSDOCID: <EP 1942698A1 >

IPR2025-01572
Apple EX1002 Page 880

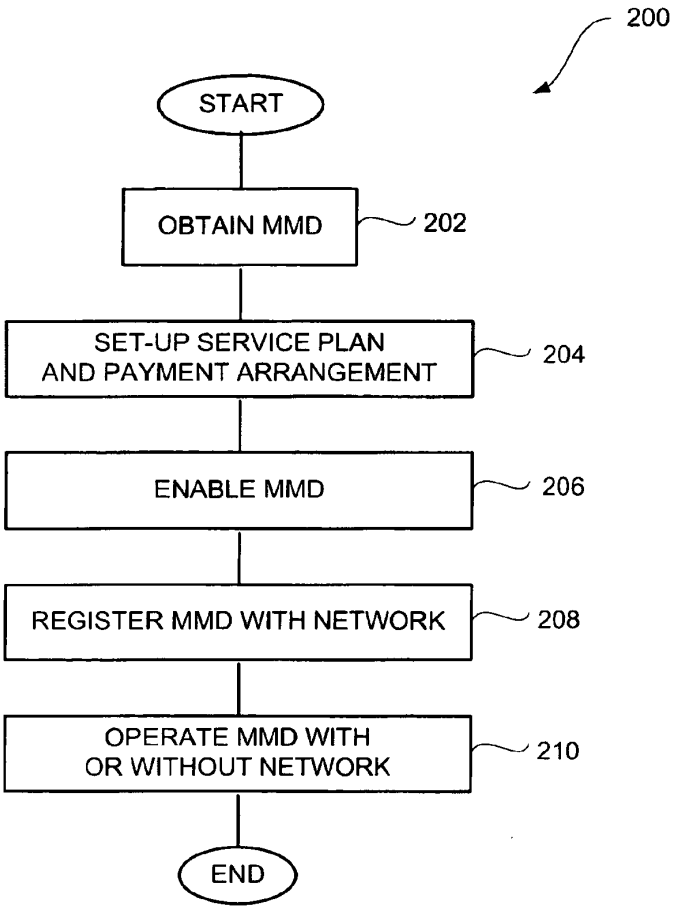


FIG. 2A

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 881

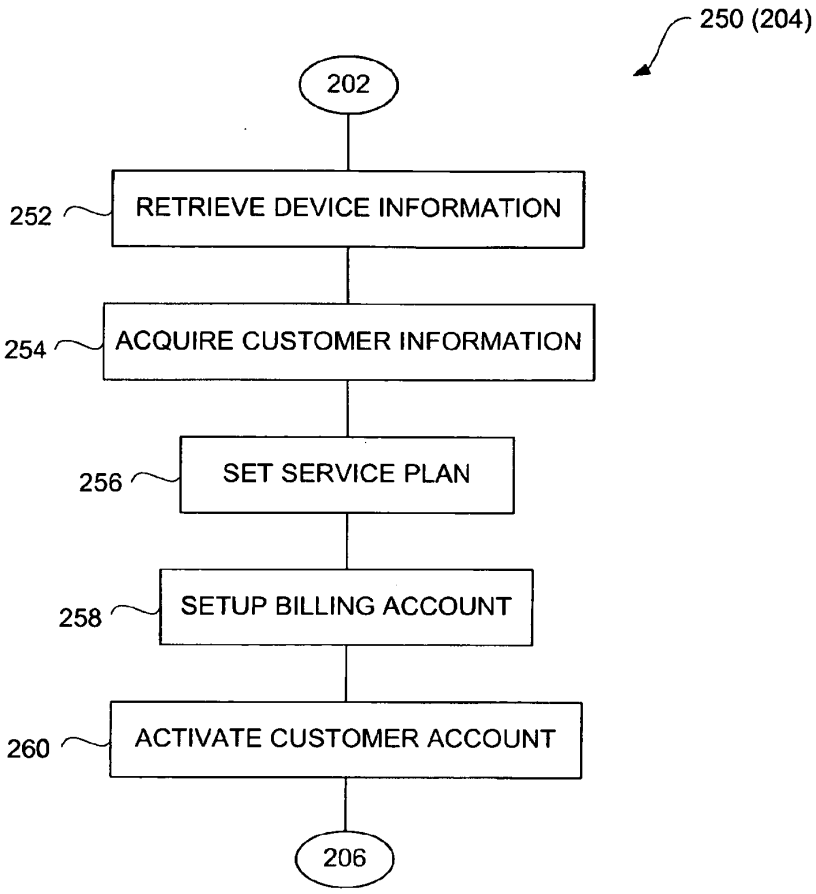


FIG. 2B

IPR2025-01572
Apple EX1002 Page 882

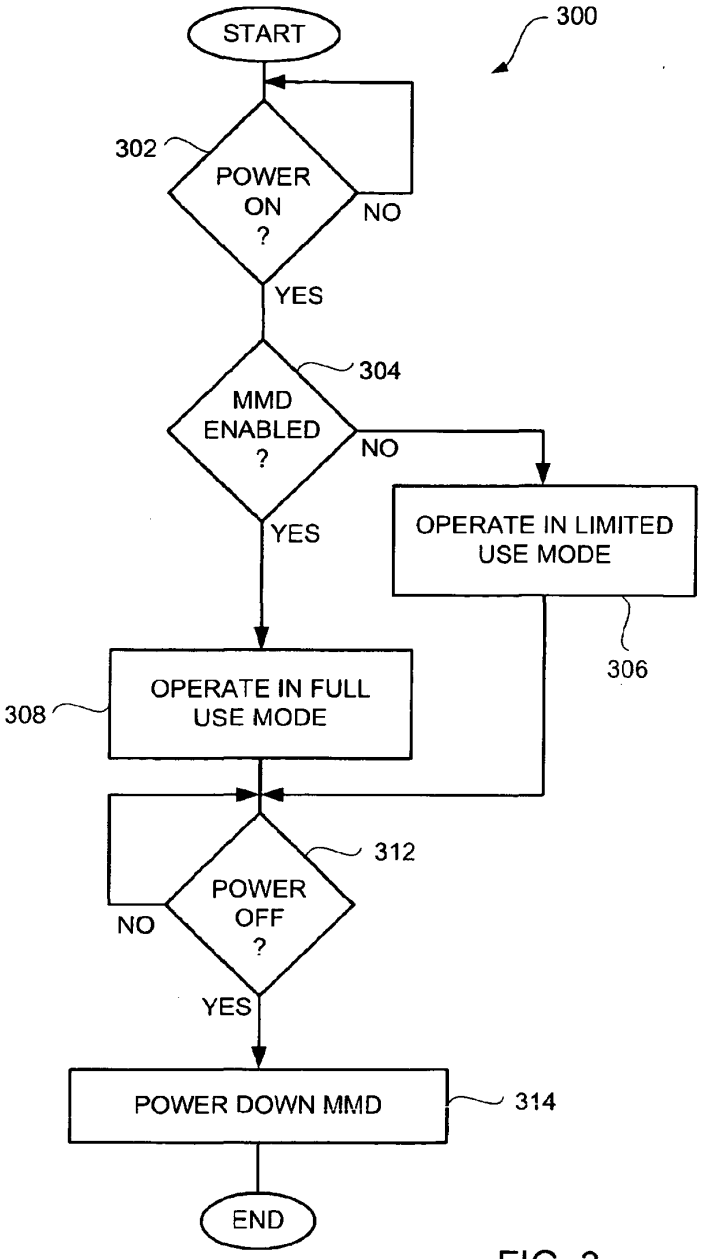


FIG. 3

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 883

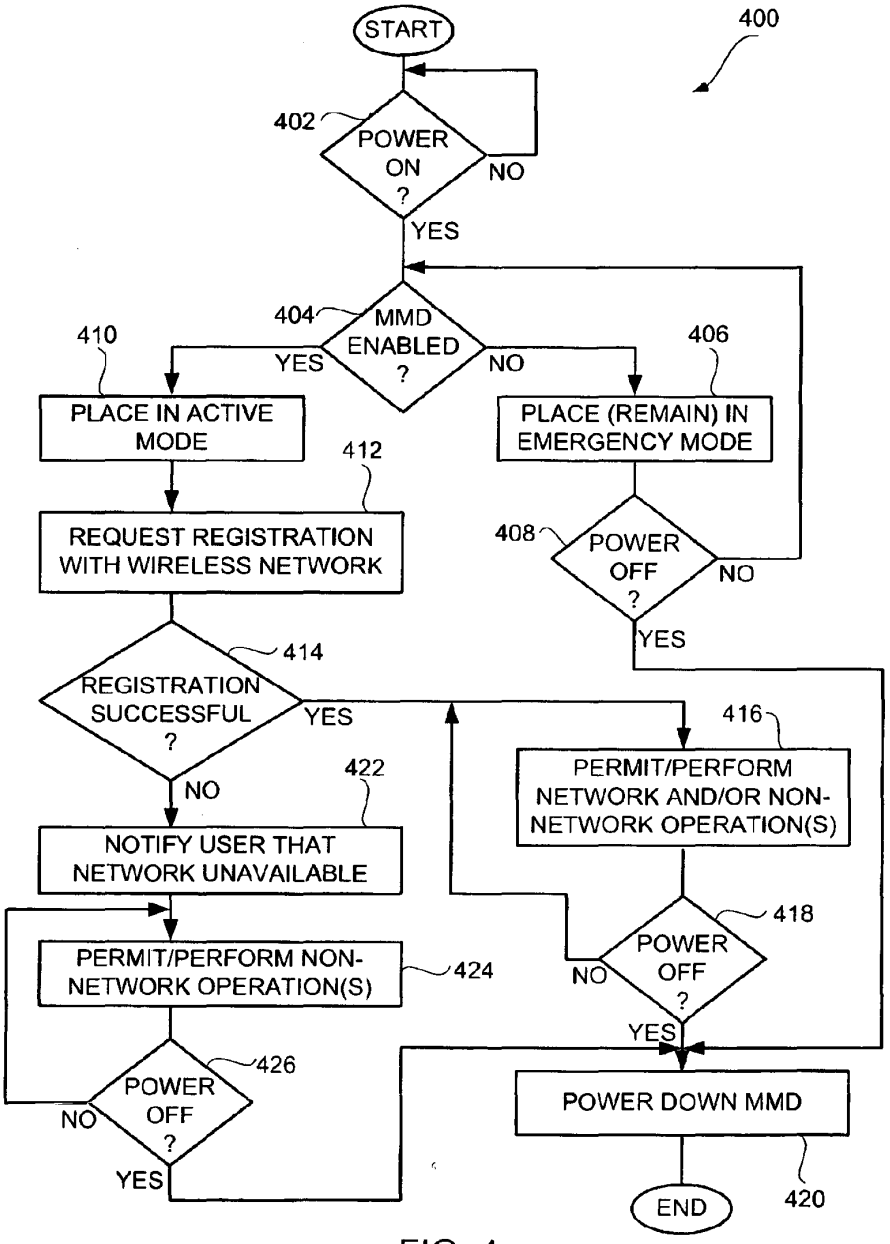


FIG. 4

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 884

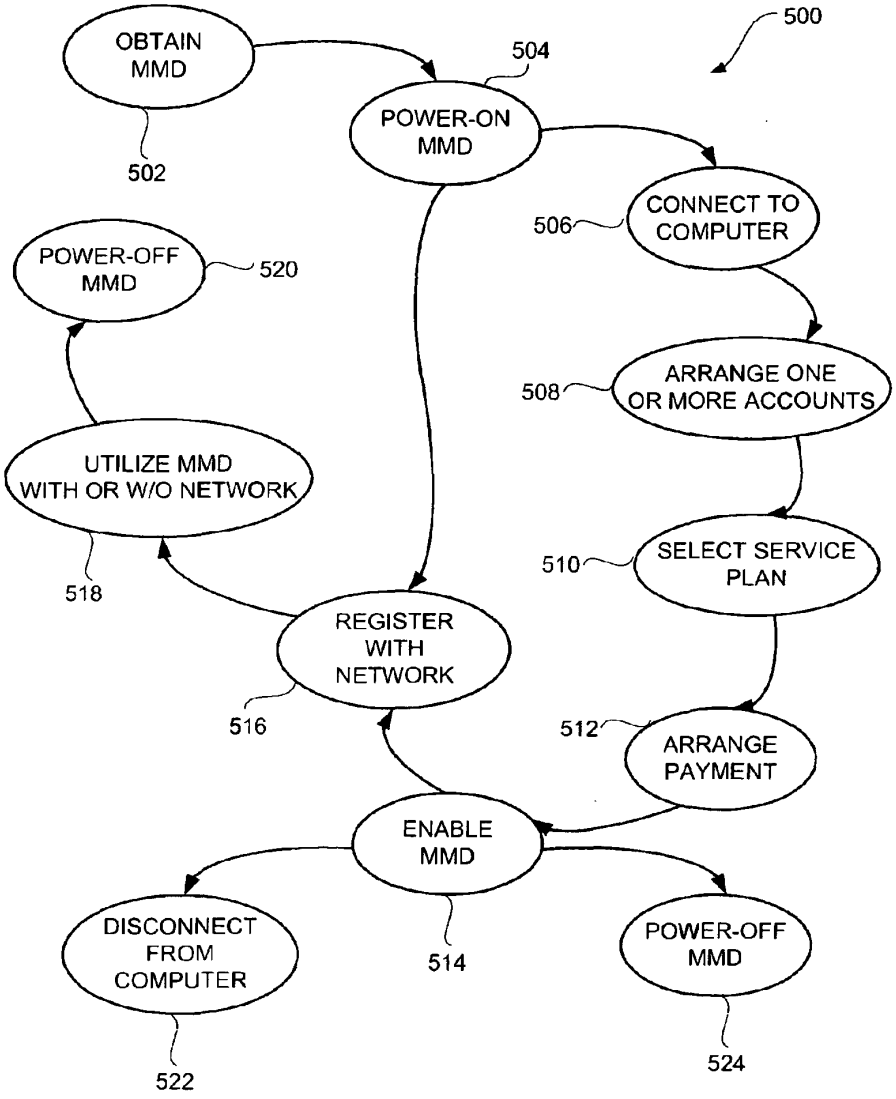


FIG. 5

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 885

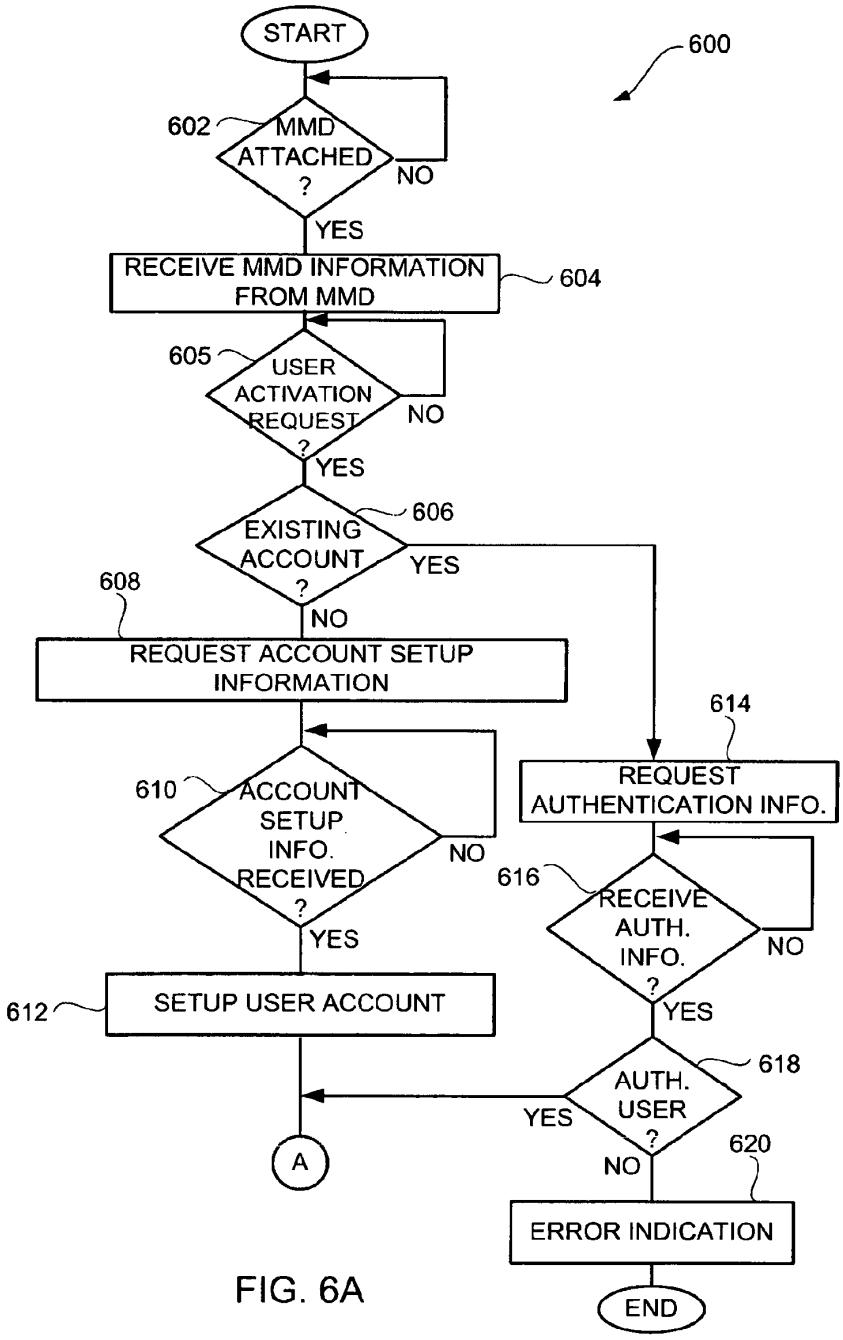


FIG. 6A

EPNSDOCID: <EP 1942698A1 | >

IPR2025-01572
Apple EX1002 Page 886

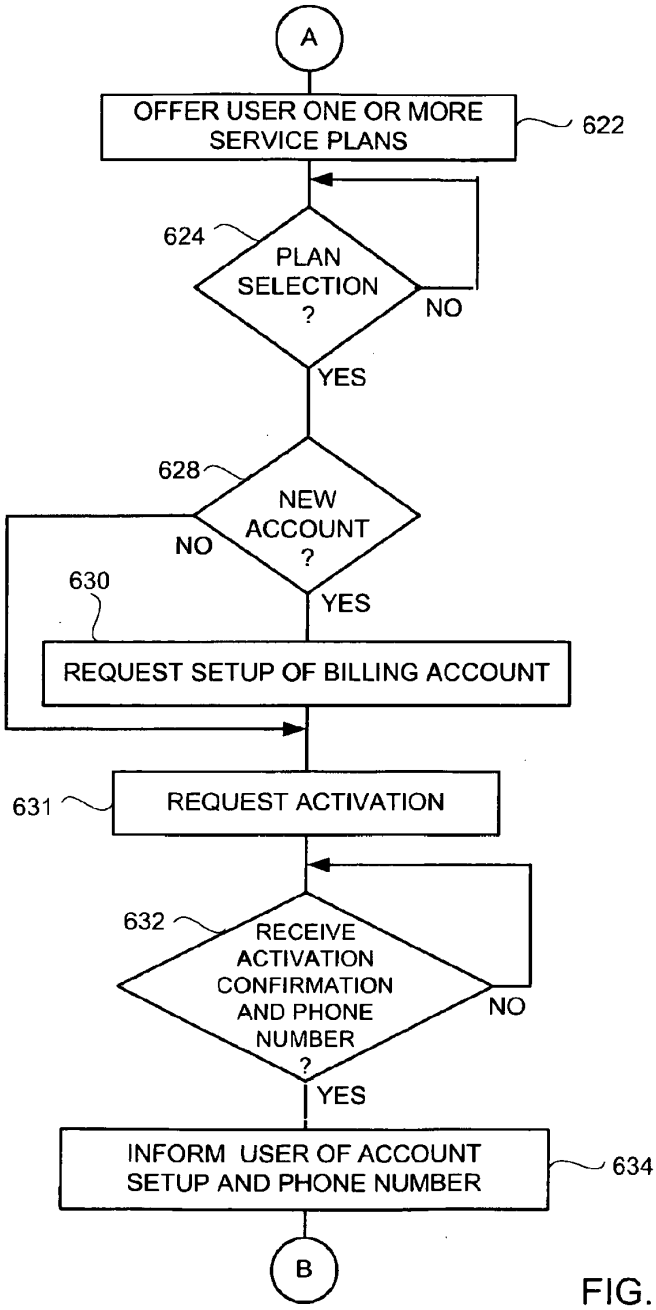


FIG. 6B

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 887

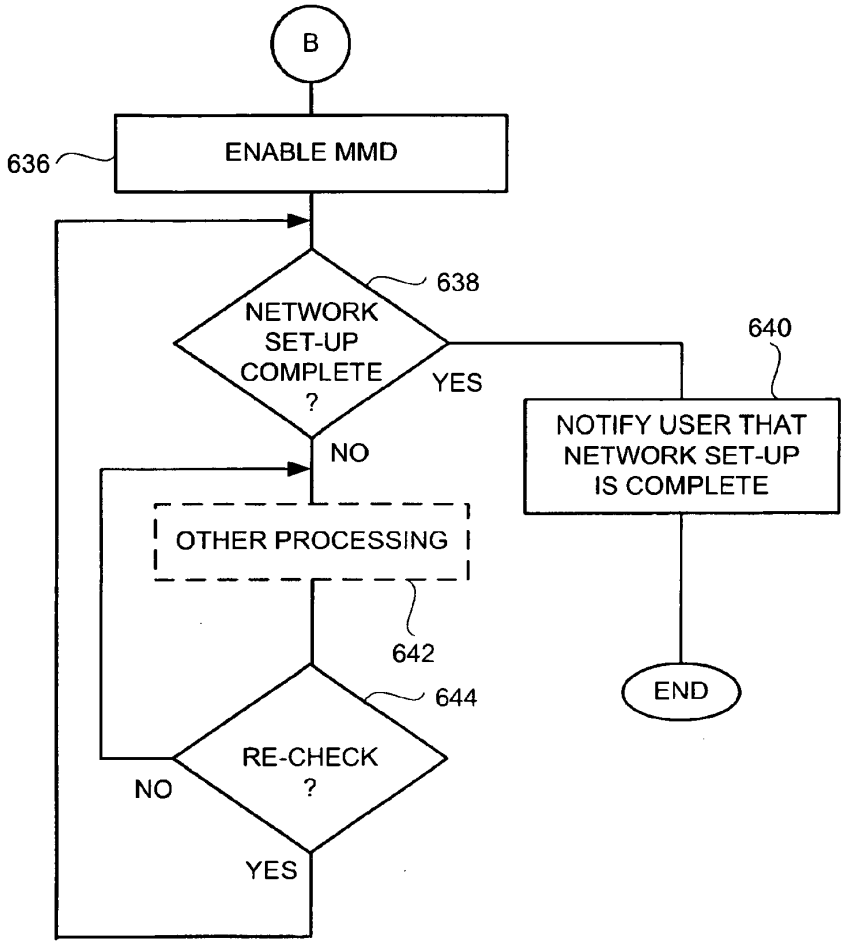


FIG. 6C

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 888

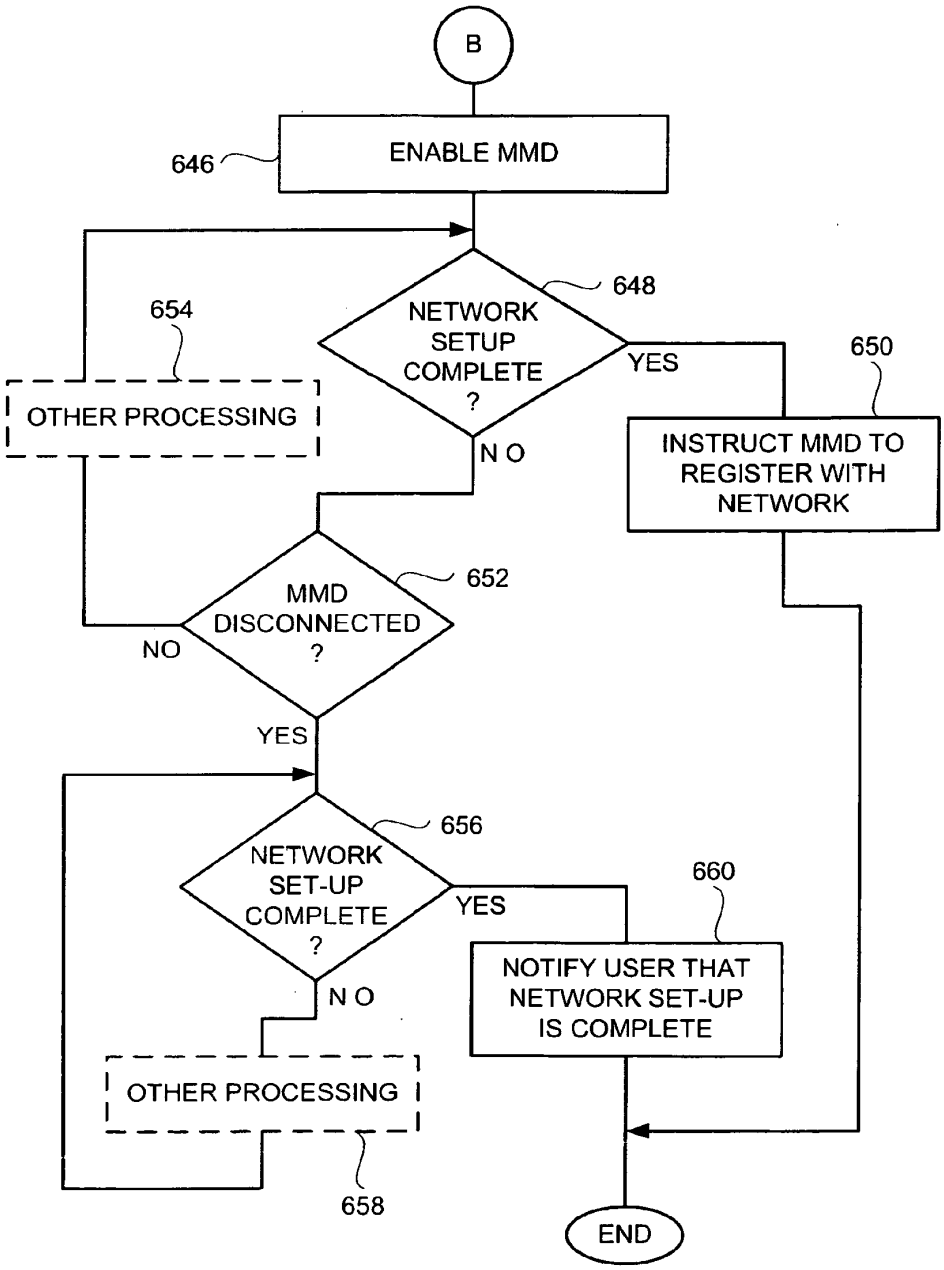


FIG. 6D

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 889

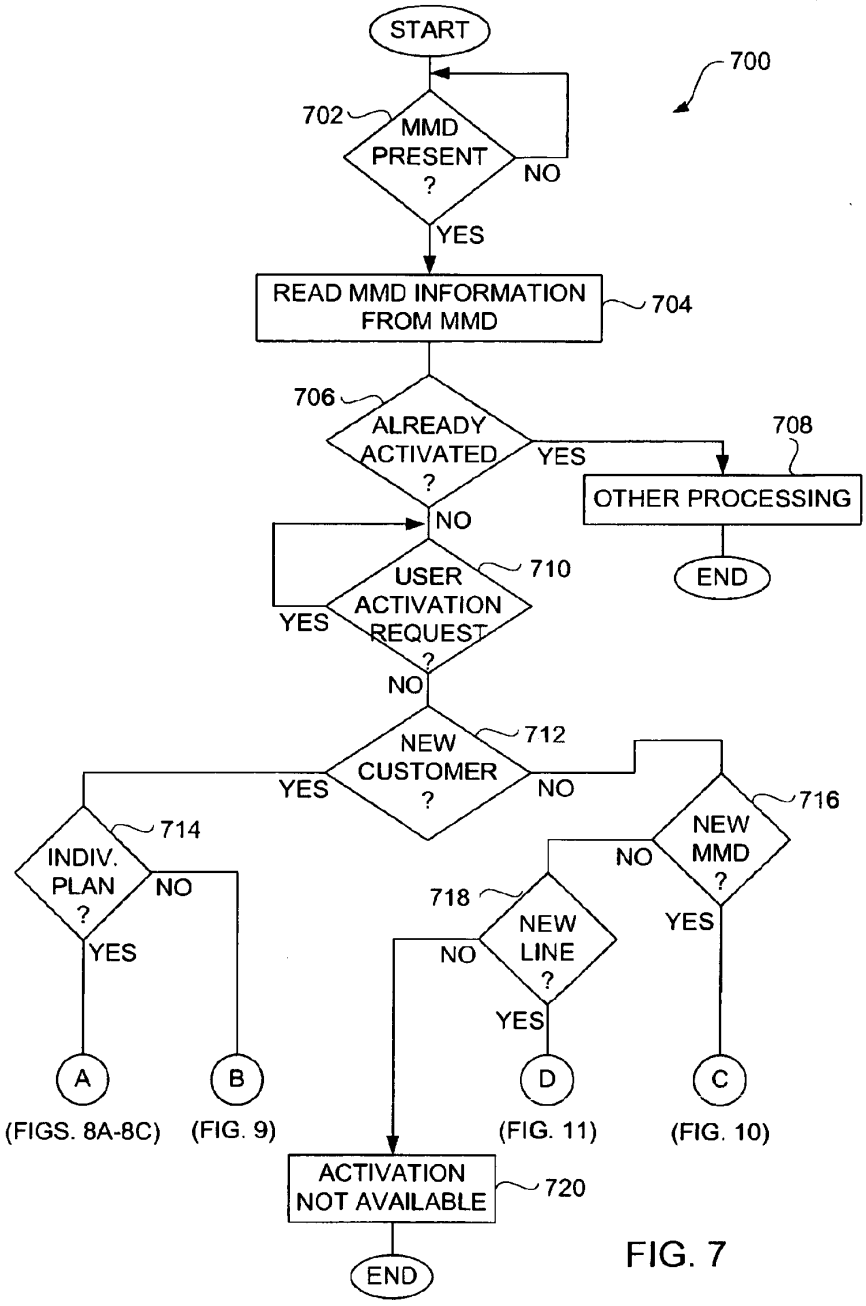


FIG. 7

IPR2025-01572
Apple EX1002 Page 890

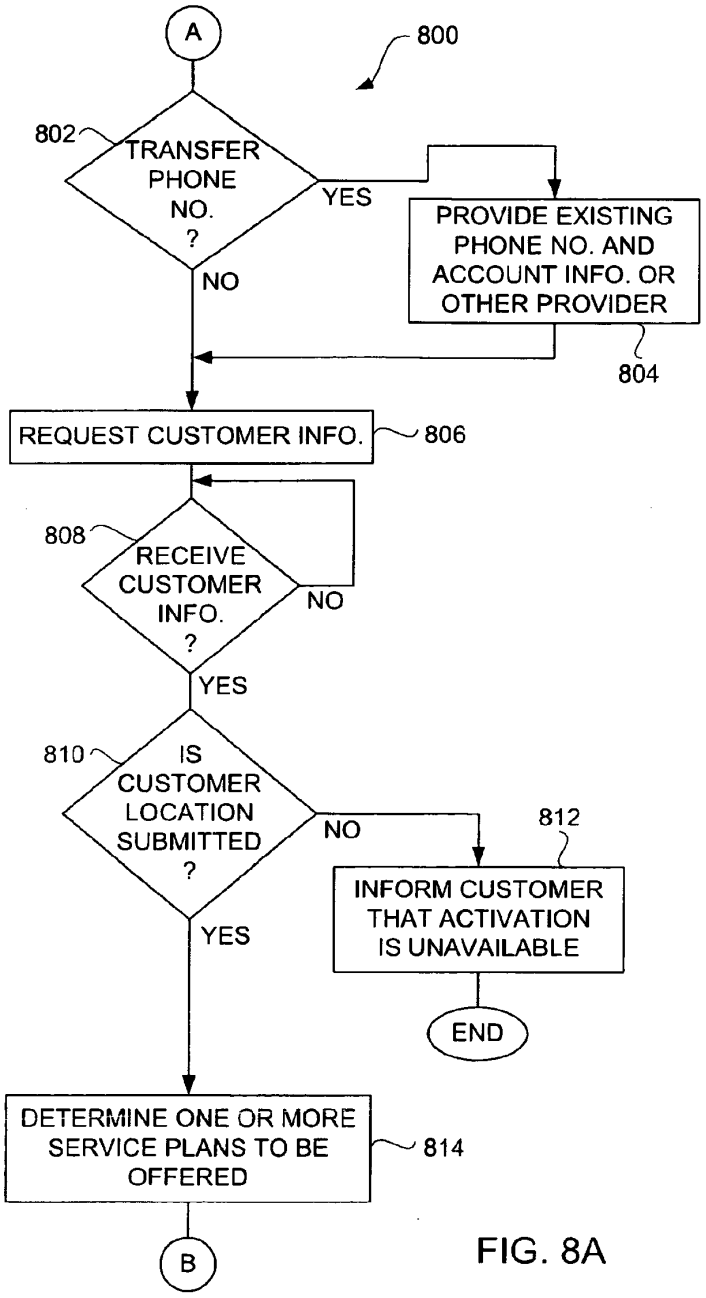


FIG. 8A

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 891

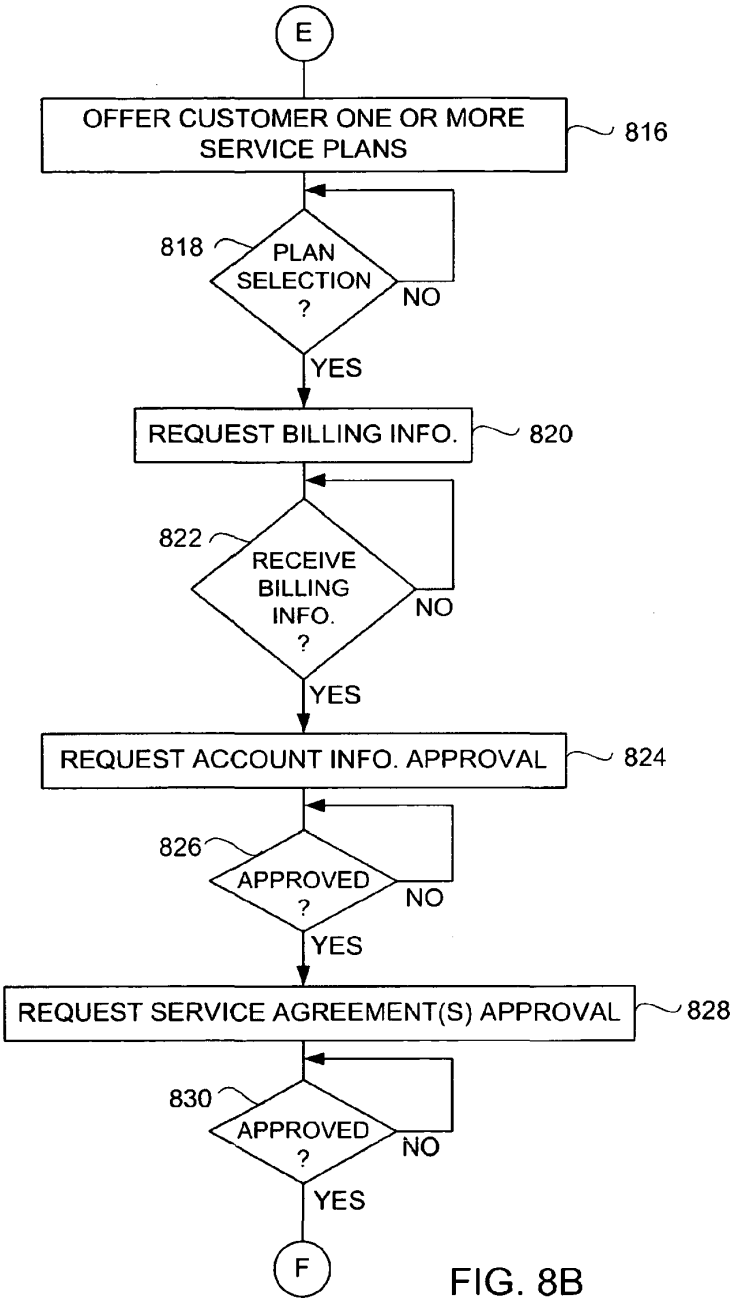


FIG. 8B

IPR2025-01572
Apple EX1002 Page 892

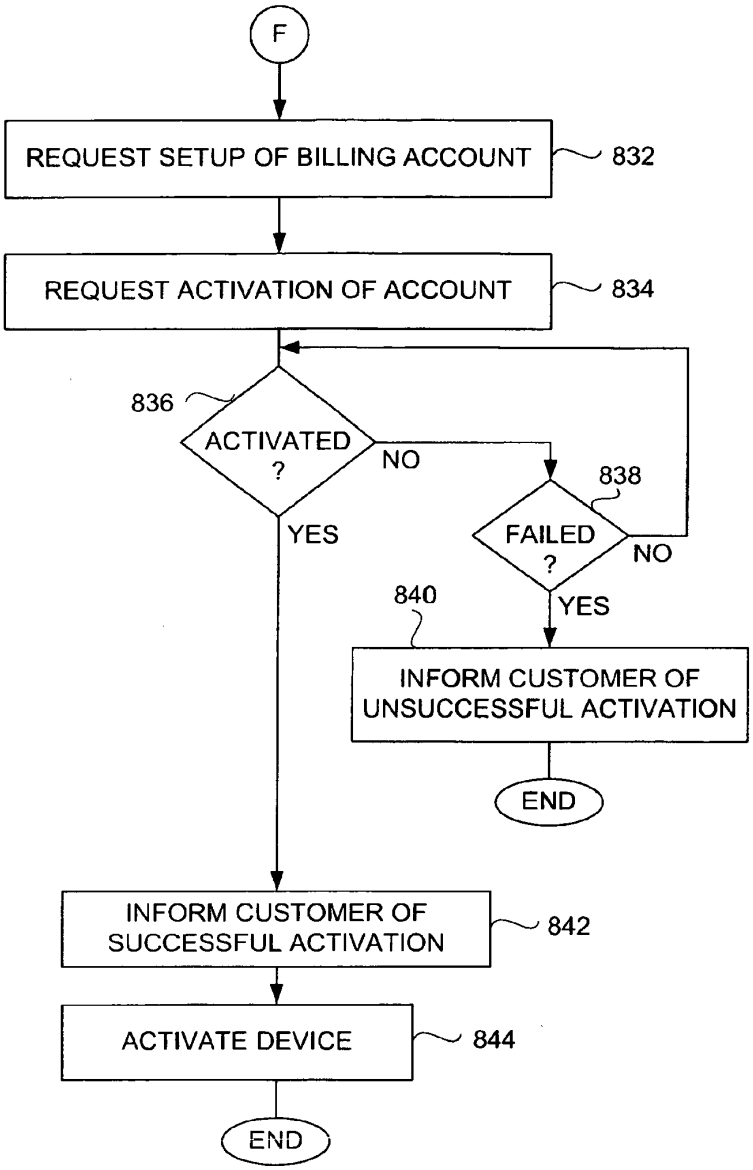


FIG. 8C

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 893

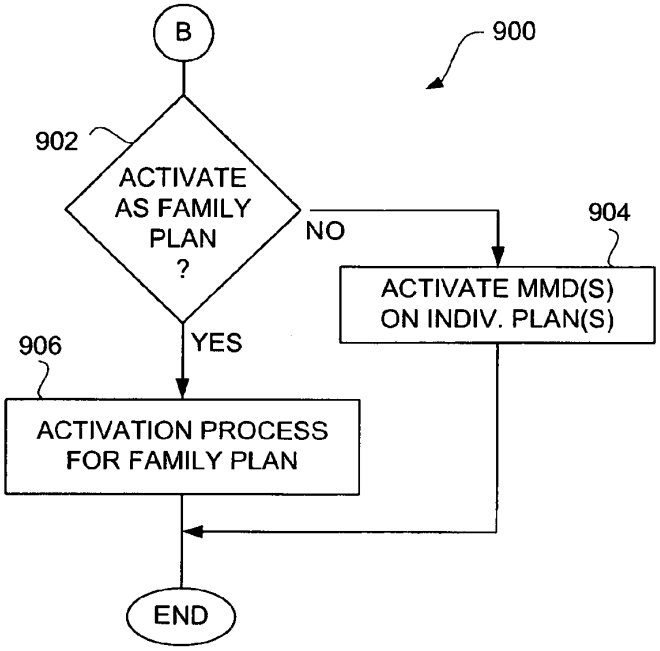


FIG. 9

IPR2025-01572
Apple EX1002 Page 894

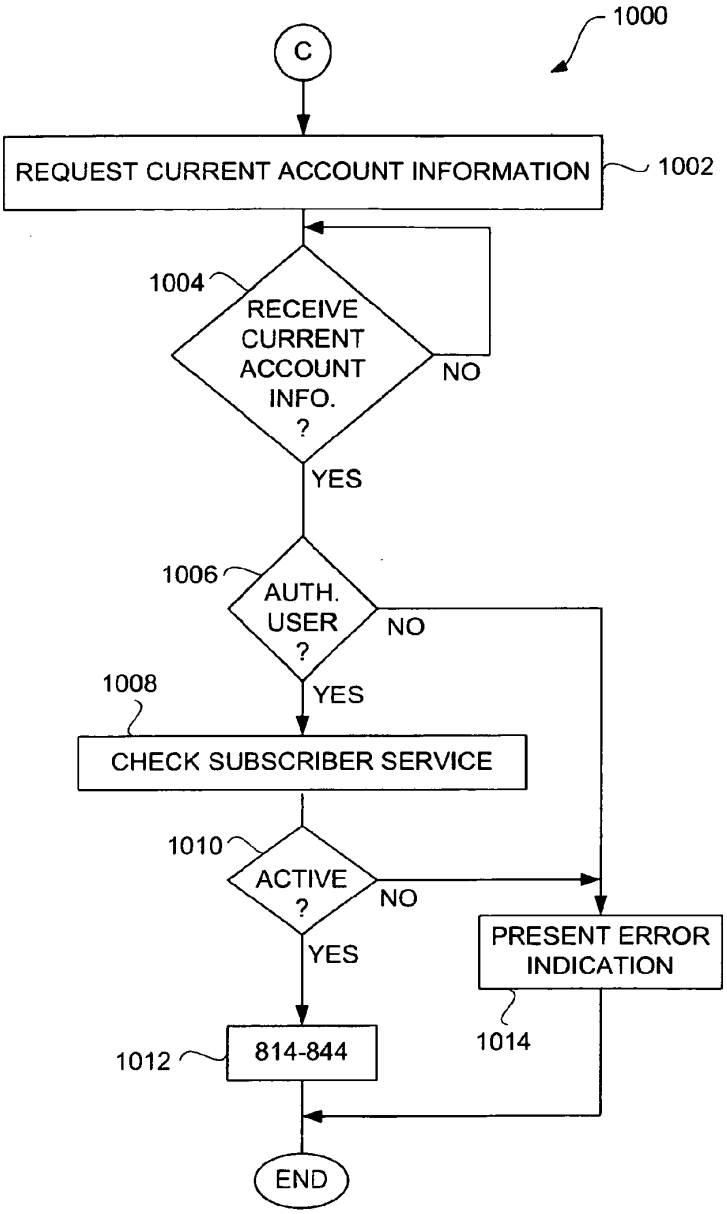


FIG. 10

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 895

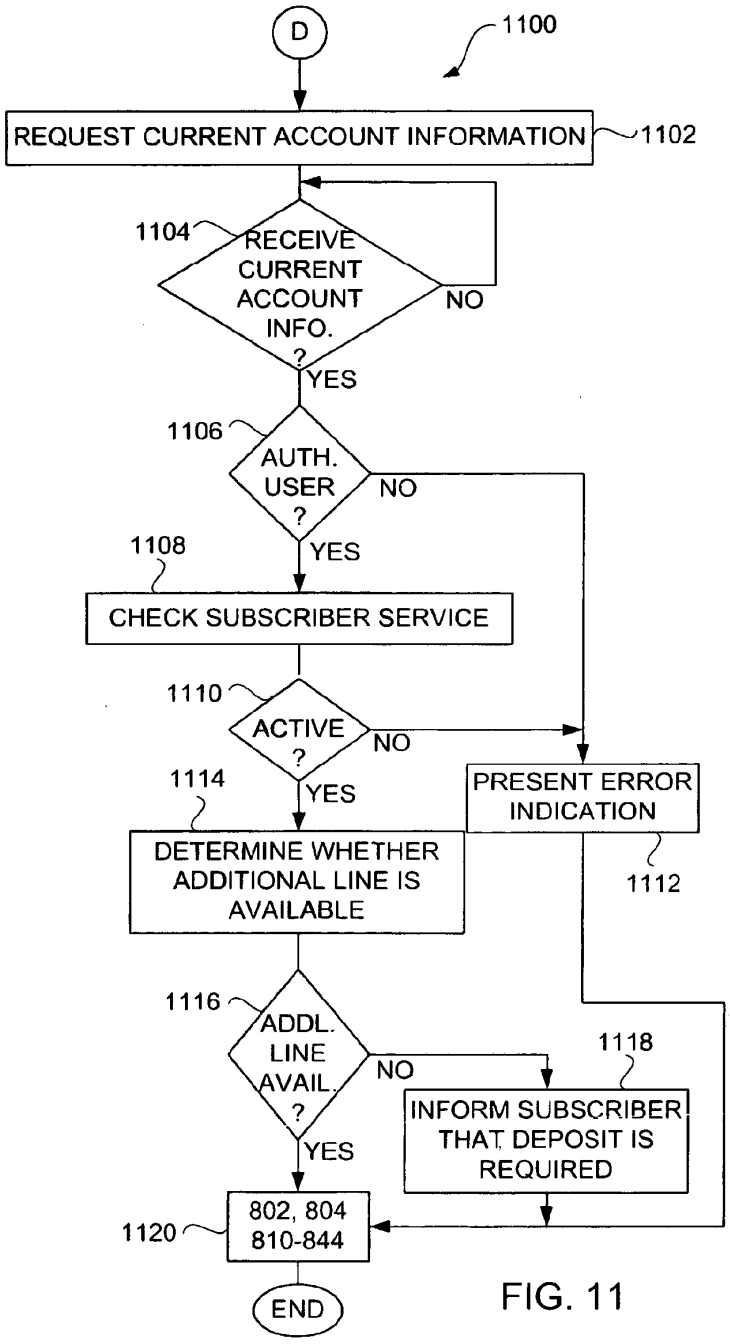


FIG. 11

IPR2025-01572
Apple EX1002 Page 896

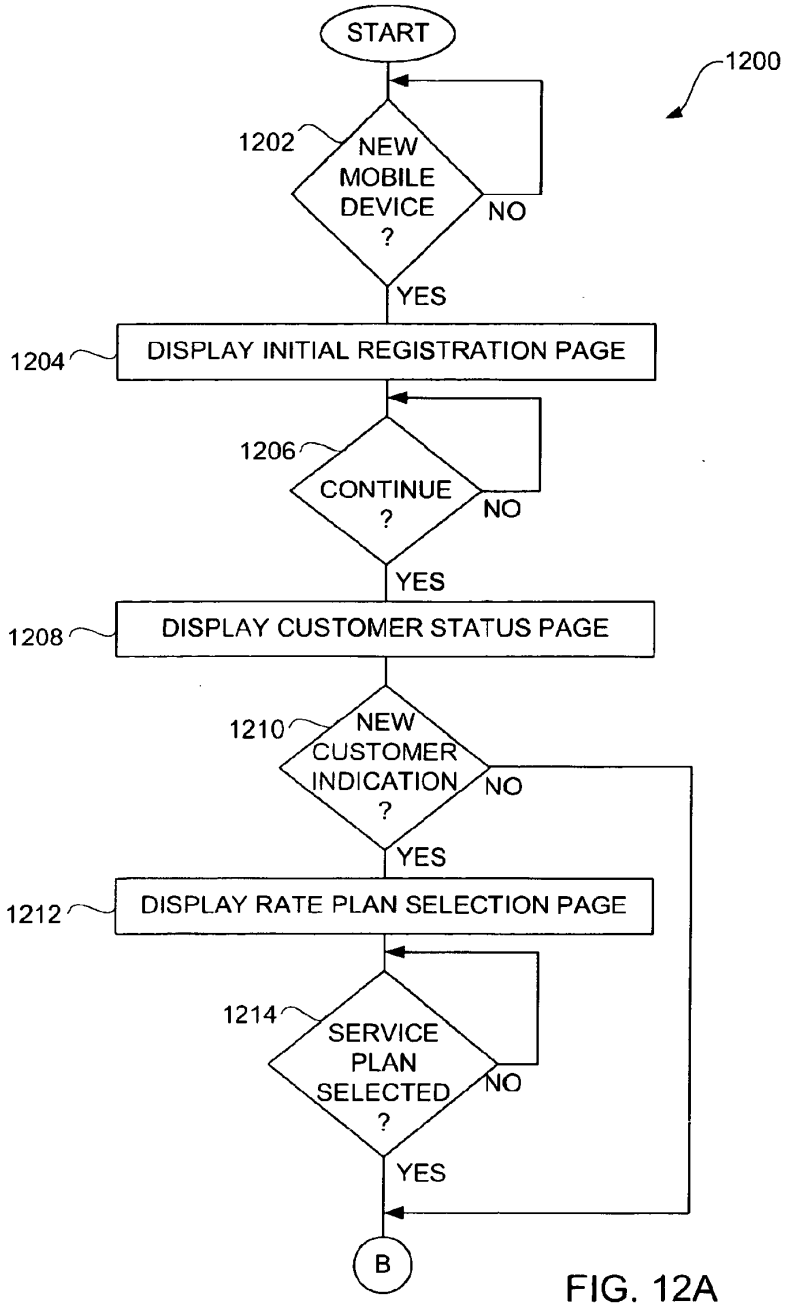


FIG. 12A

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 897

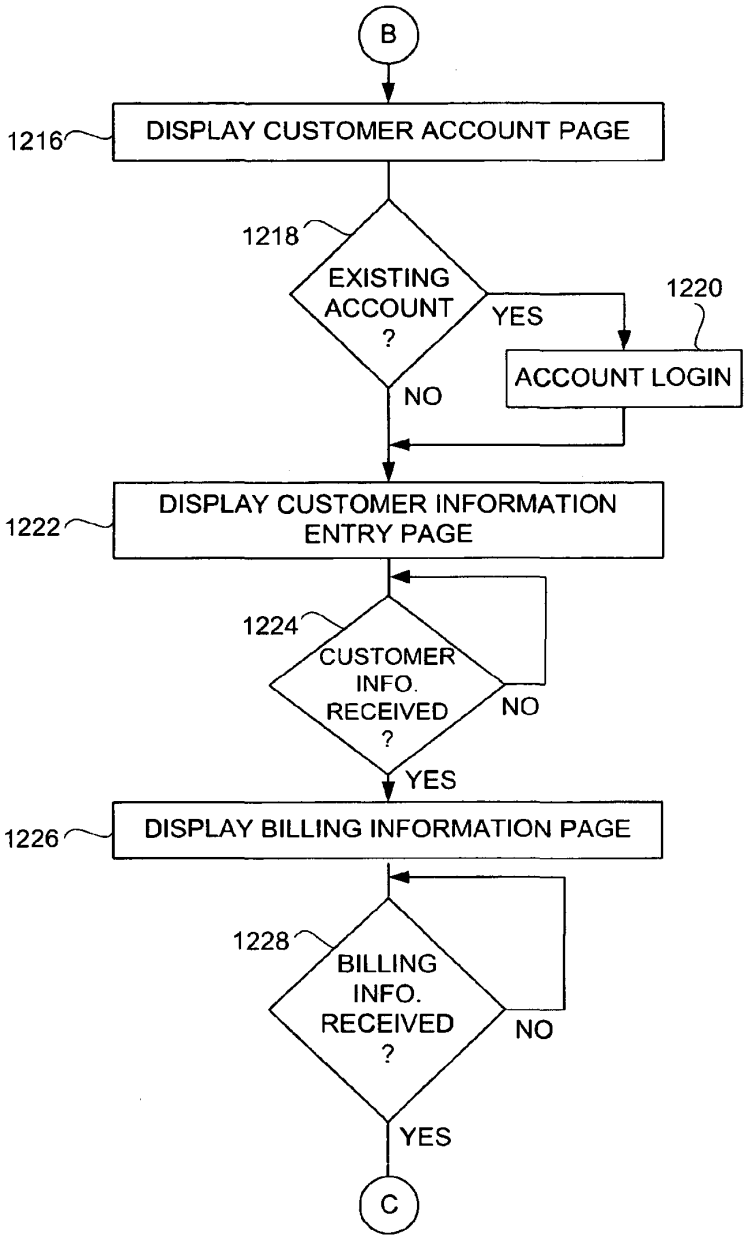


FIG. 12B

IPR2025-01572
Apple EX1002 Page 898

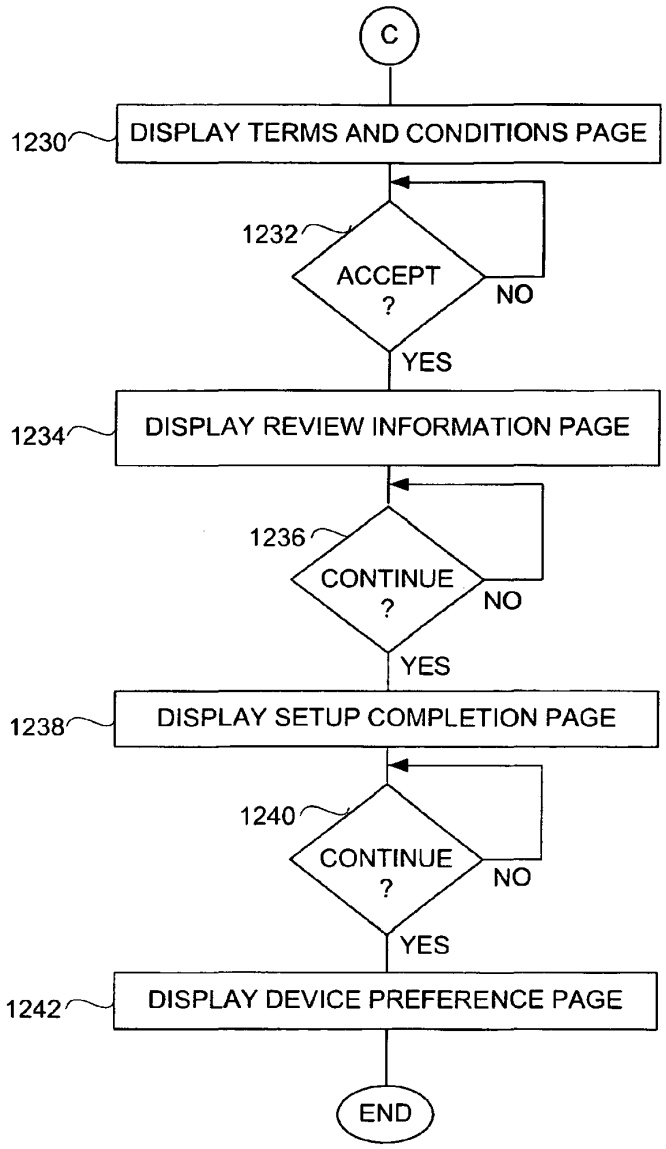


FIG. 12C

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 899

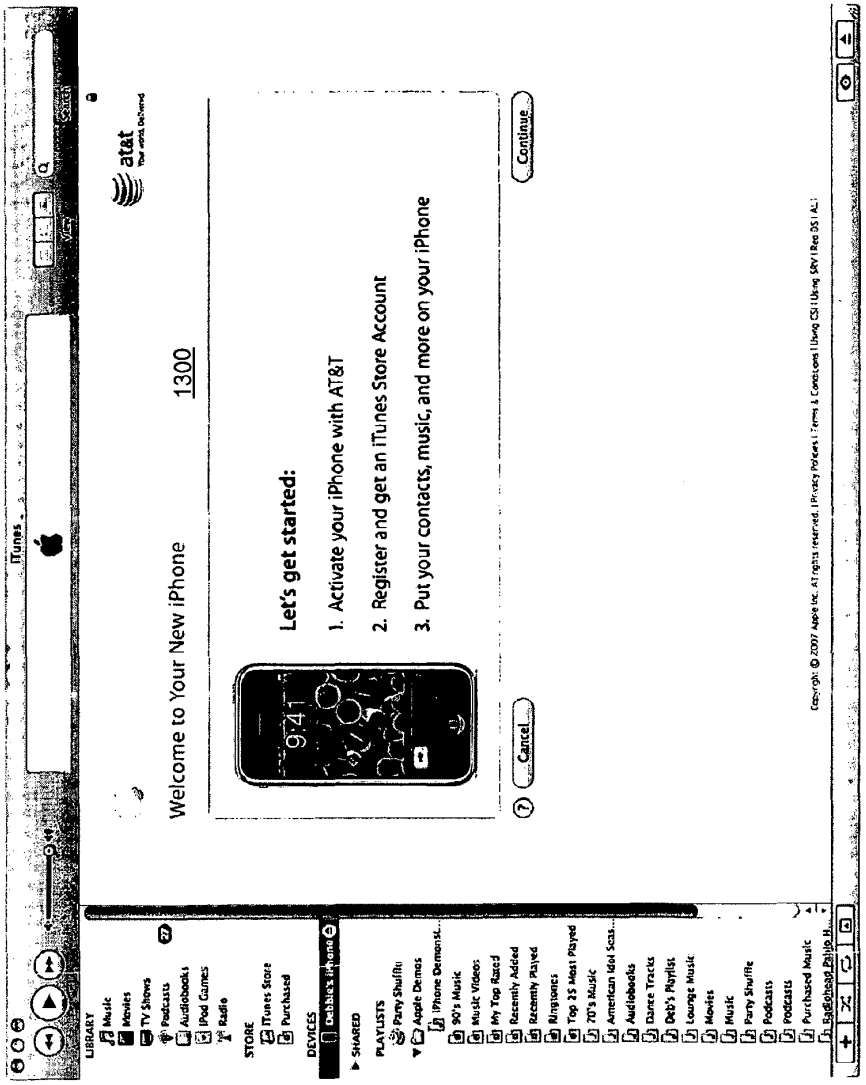


FIG. 13

IPR2025-01572
Apple EX1002 Page 900

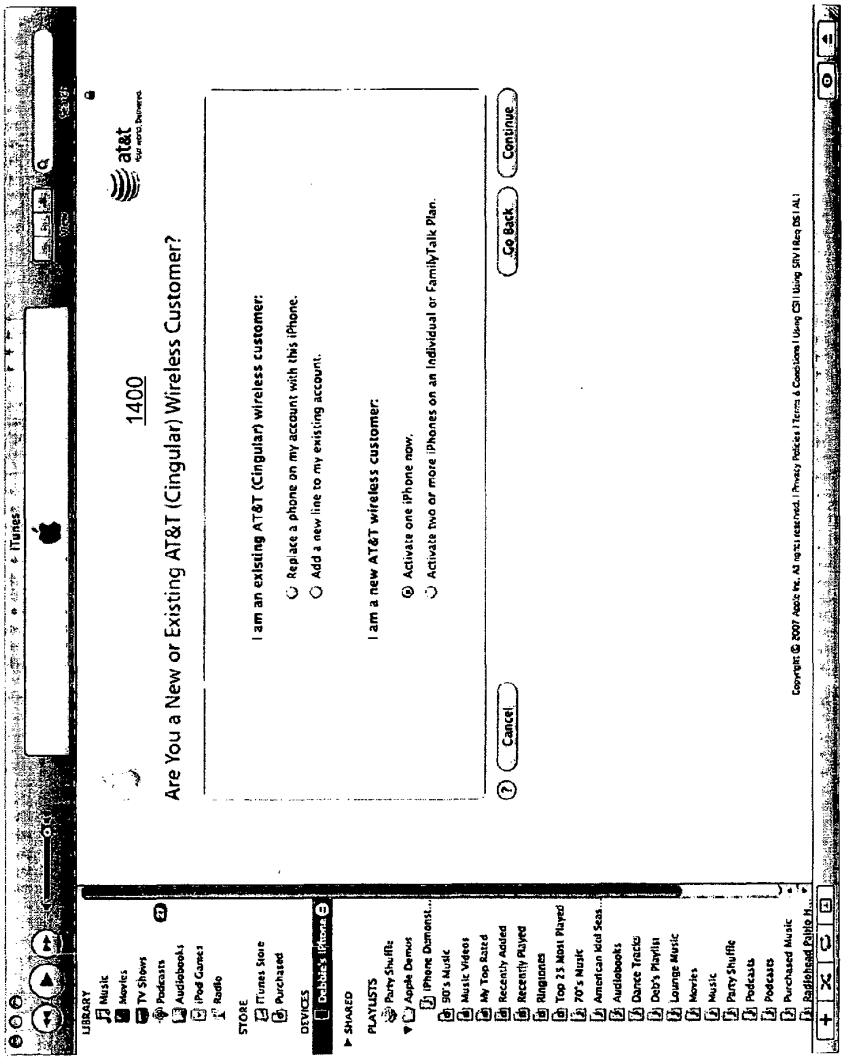


FIG. 14

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 901

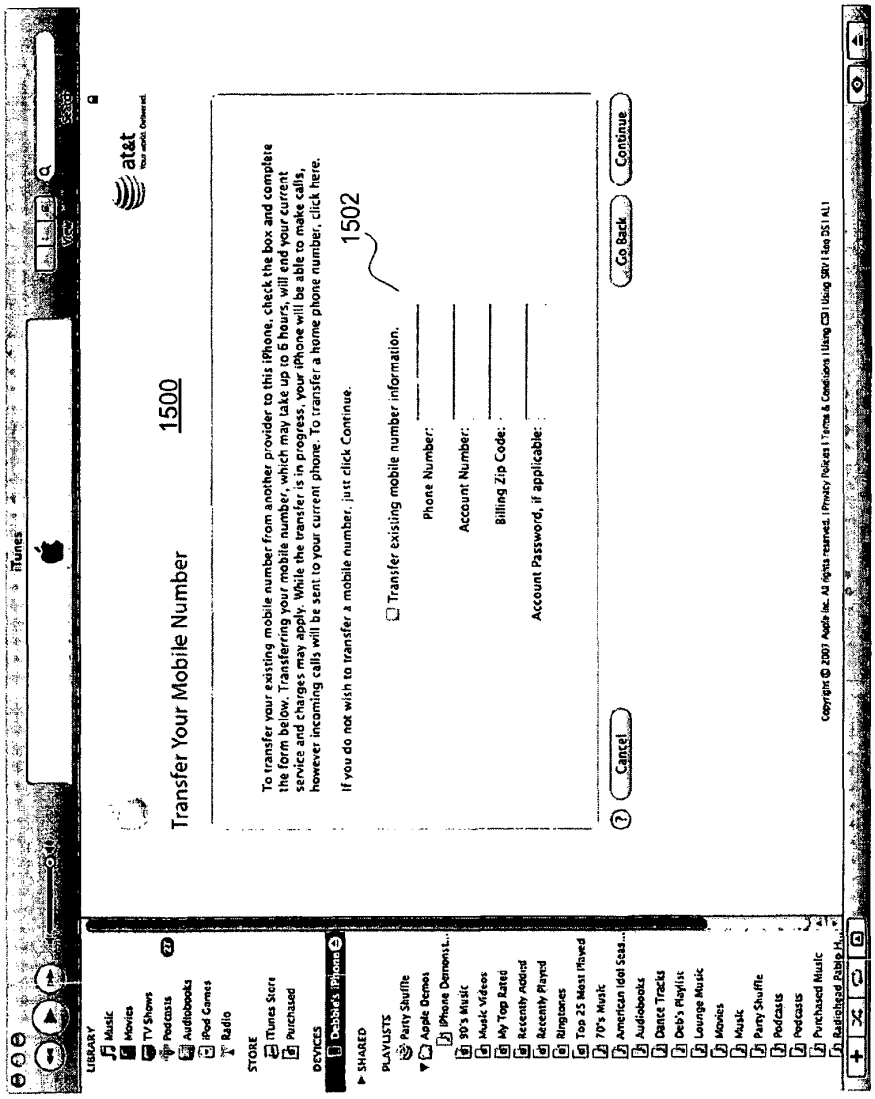


FIG. 15

IPR2025-01572
Apple EX1002 Page 902

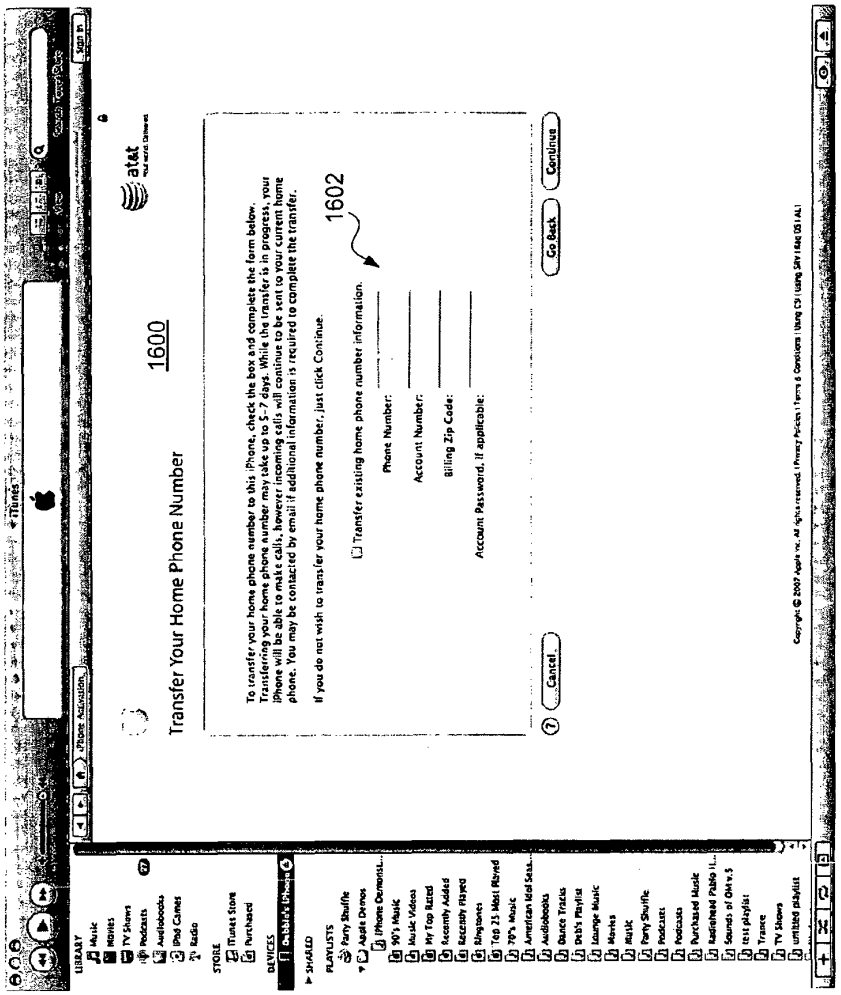


FIG. 16

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 903

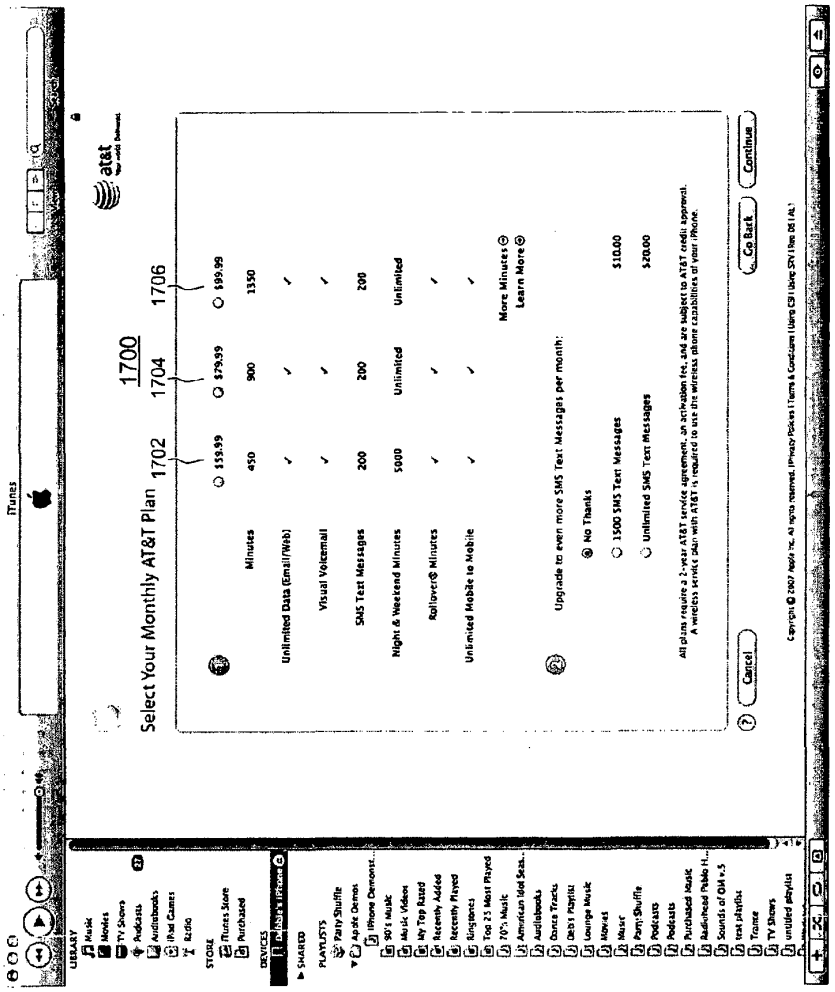


FIG. 17A

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 904

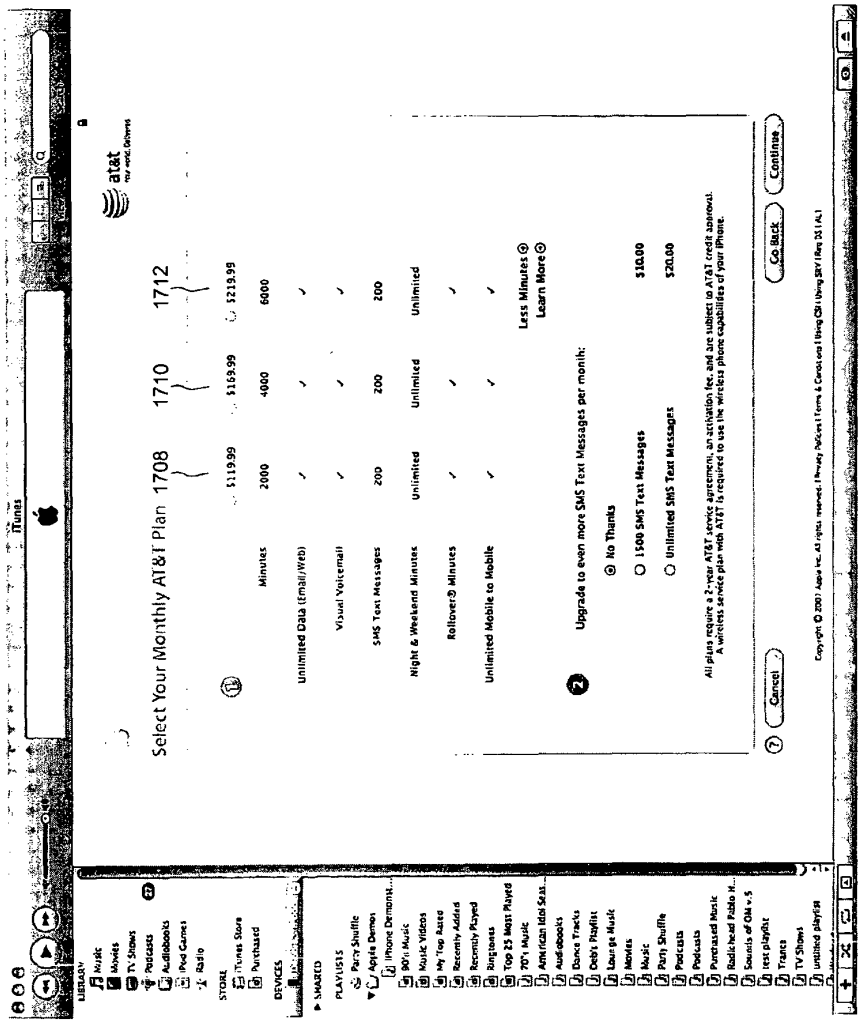


FIG. 17B

BNSDOCID: <EP._____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 905

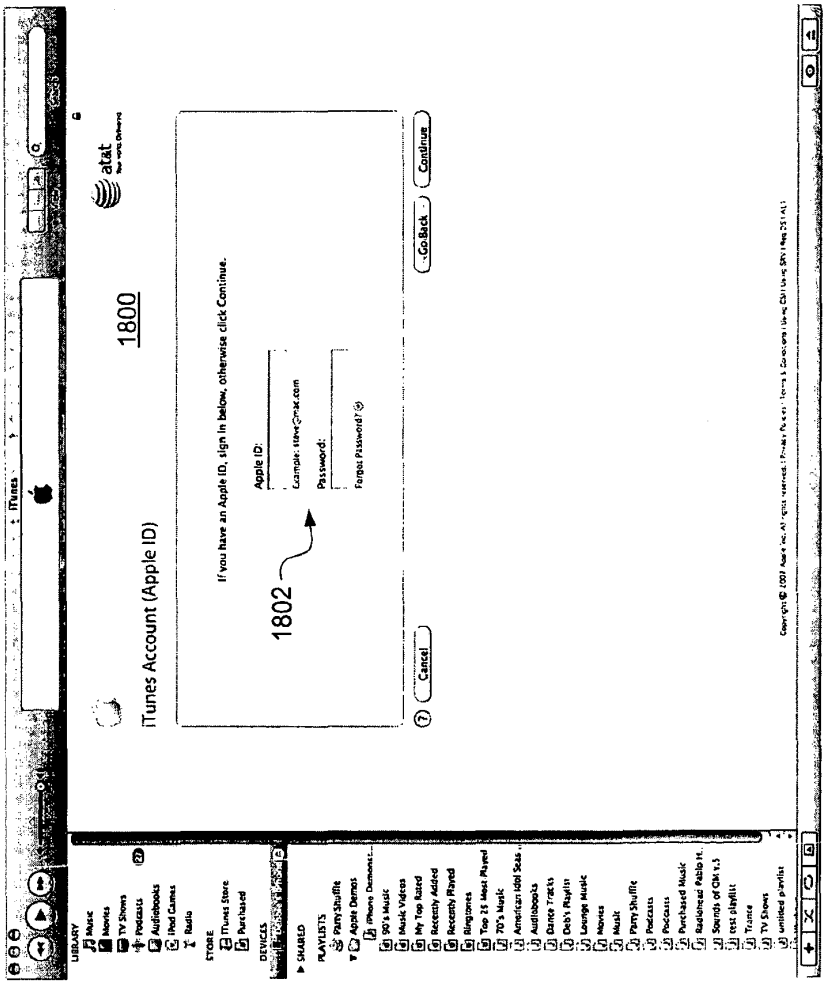


FIG. 18

EPODOC: <EP 1942698A1 >

IPR2025-01572
Apple EX1002 Page 906

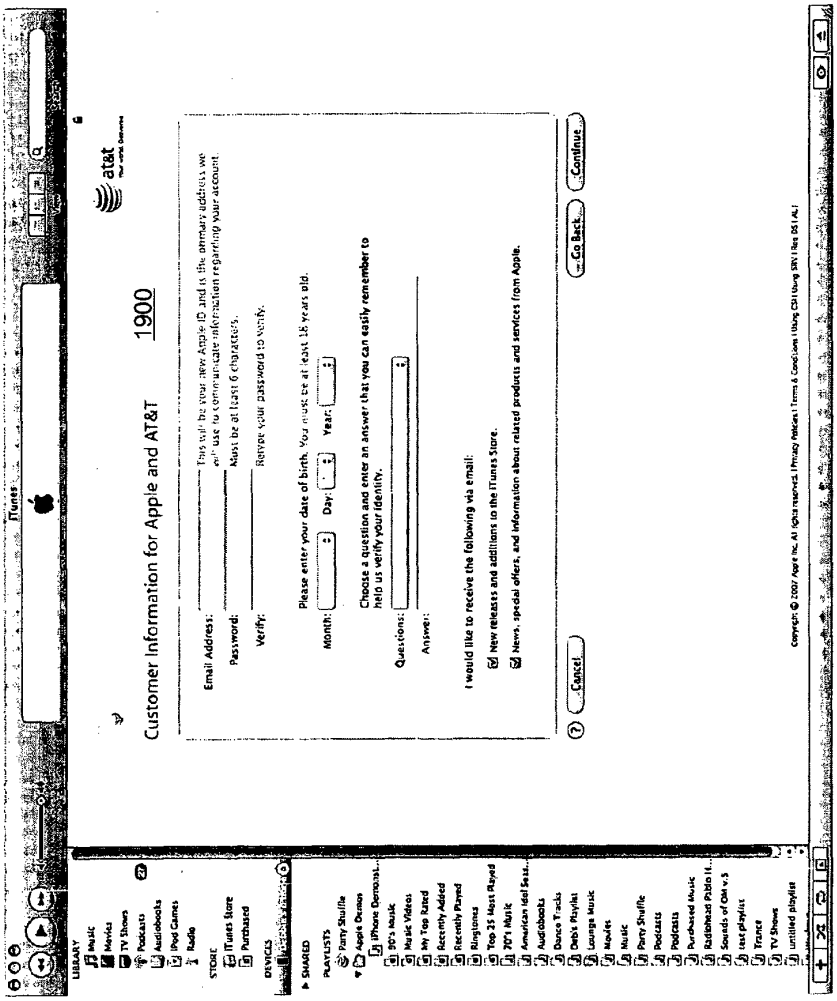


FIG. 19

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 907

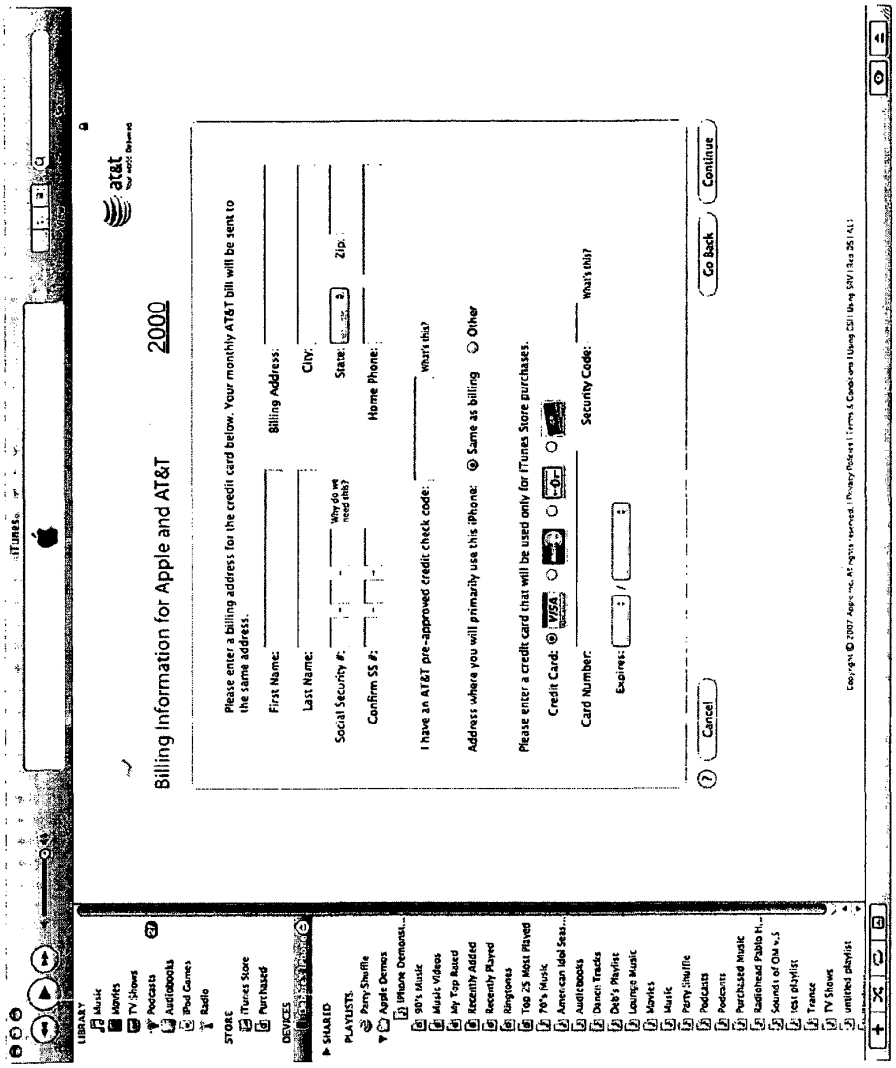


FIG. 20

IPR2025-01572
Apple EX1002 Page 908

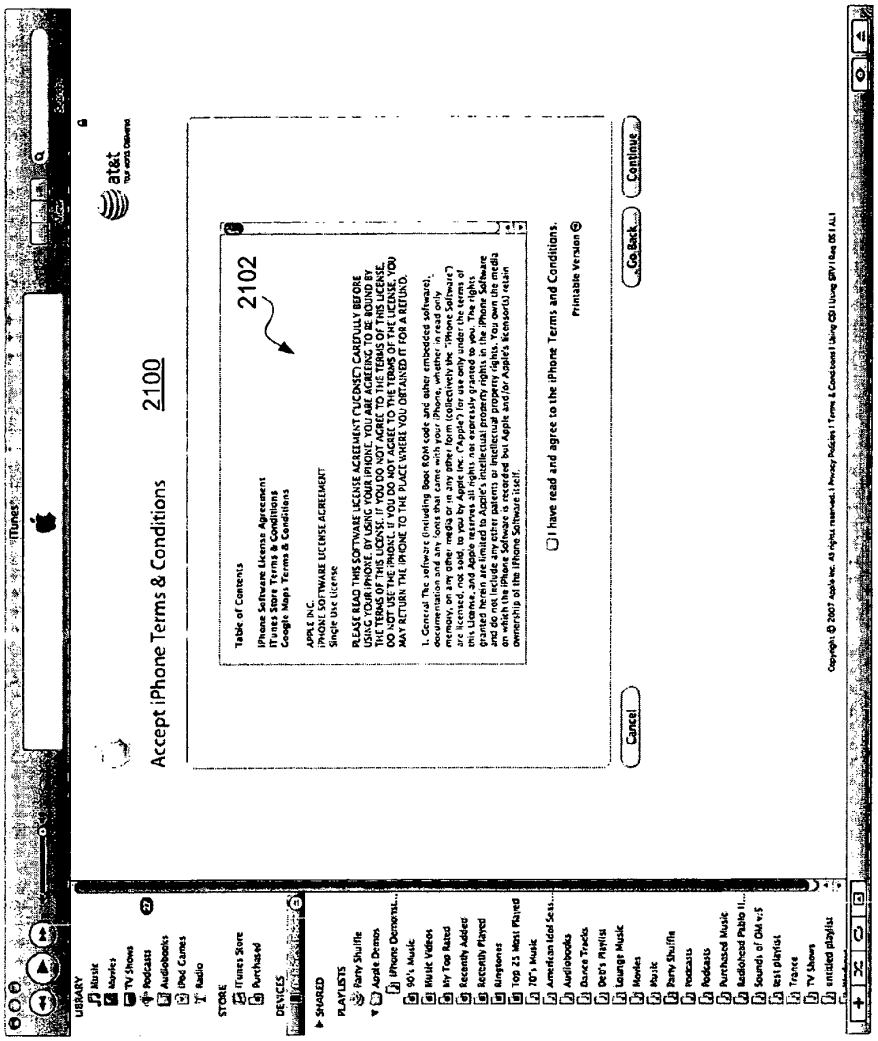


FIG. 21A

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 909

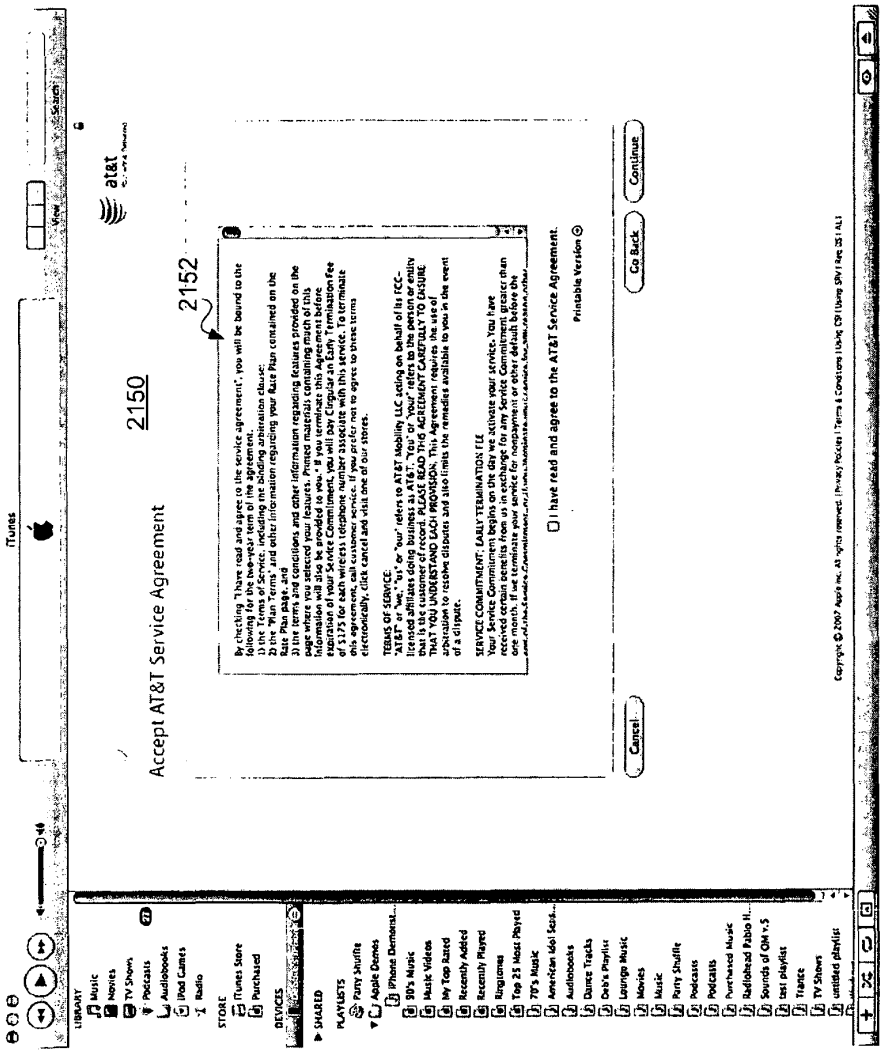


FIG. 21B

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 910

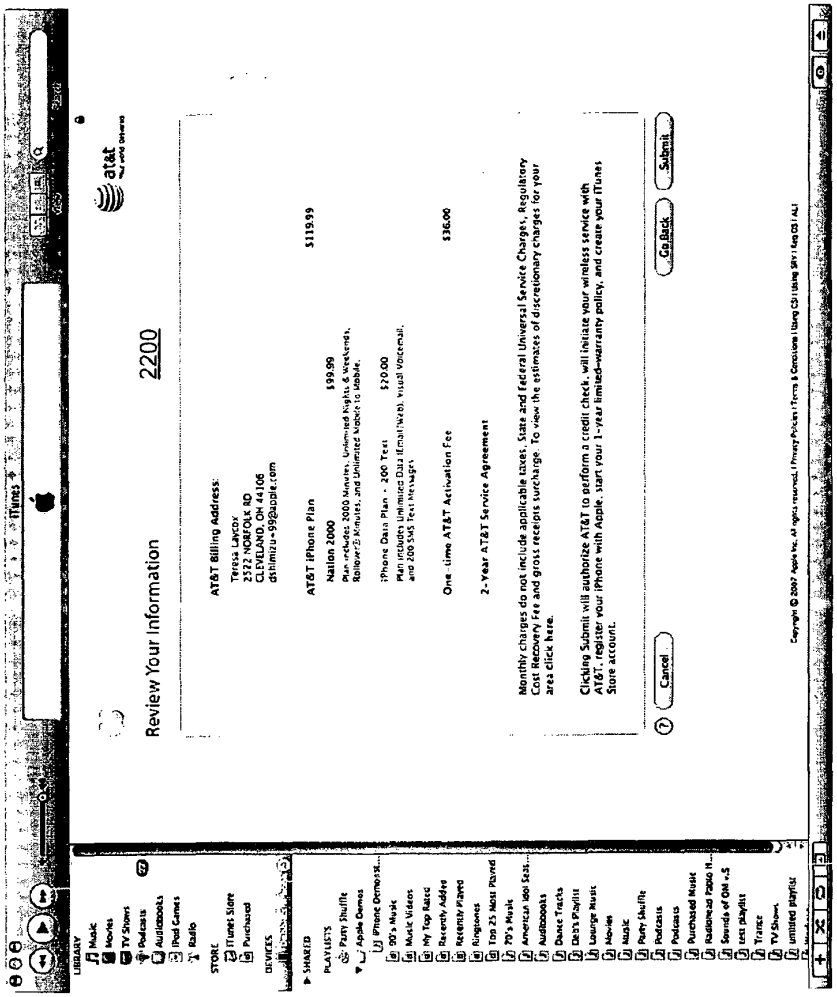


FIG. 22

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 911

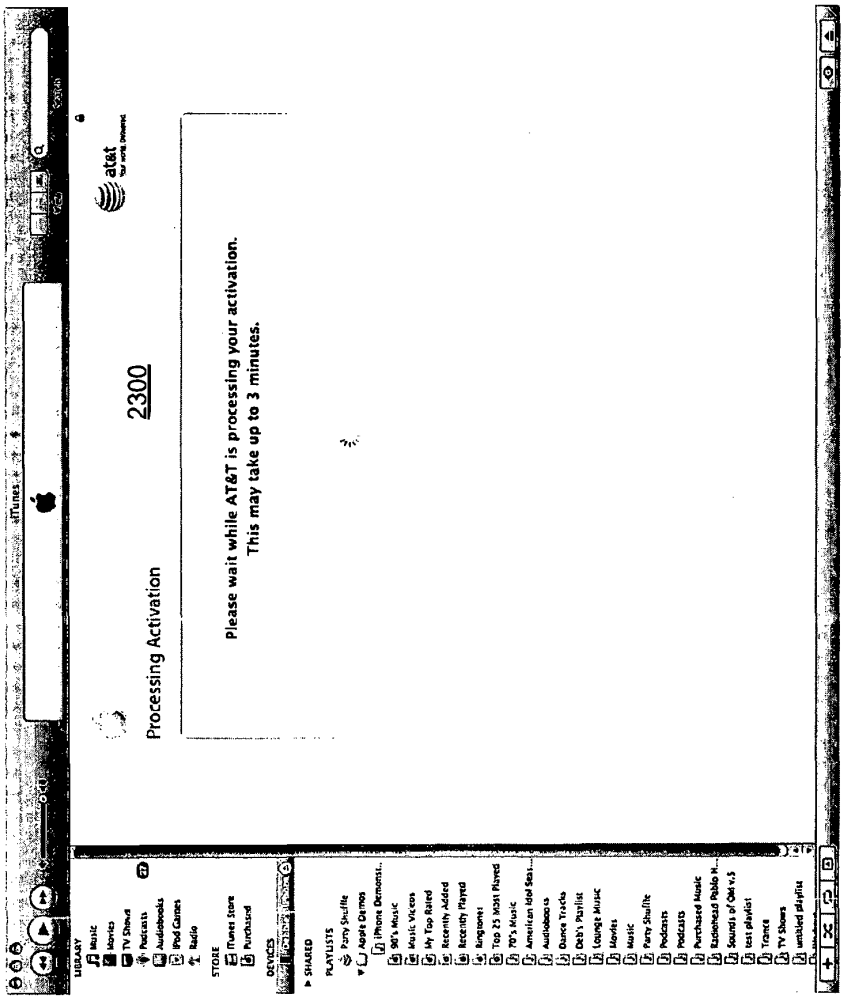


FIG. 23

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 912

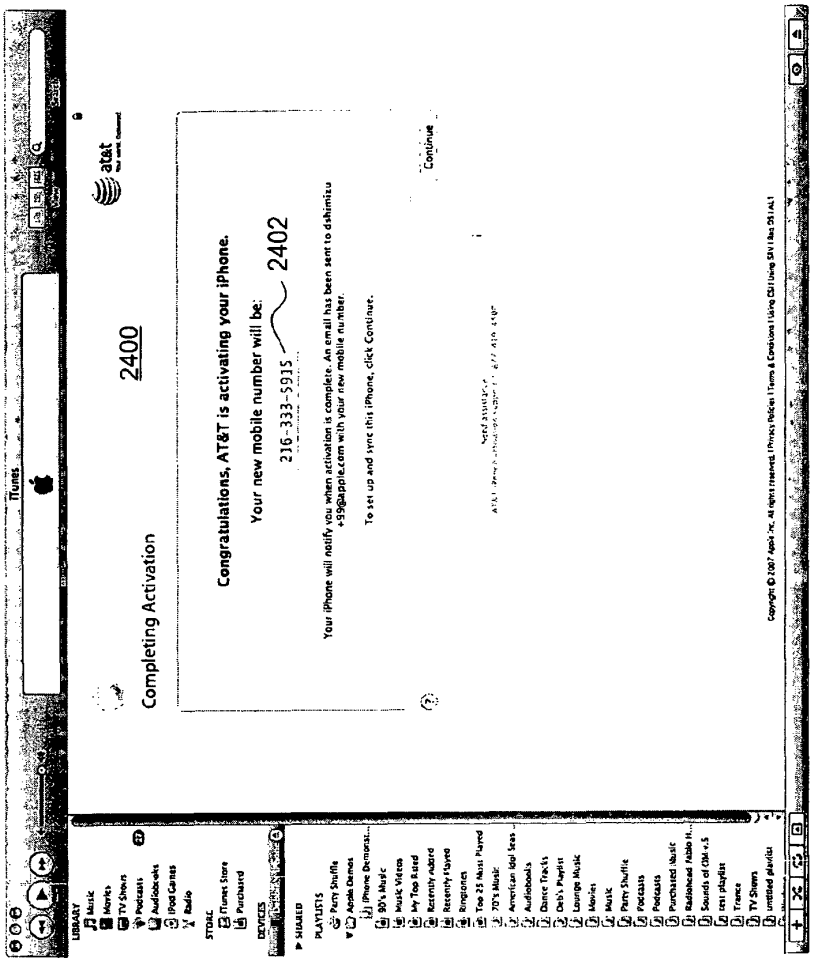


FIG. 24A

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 913

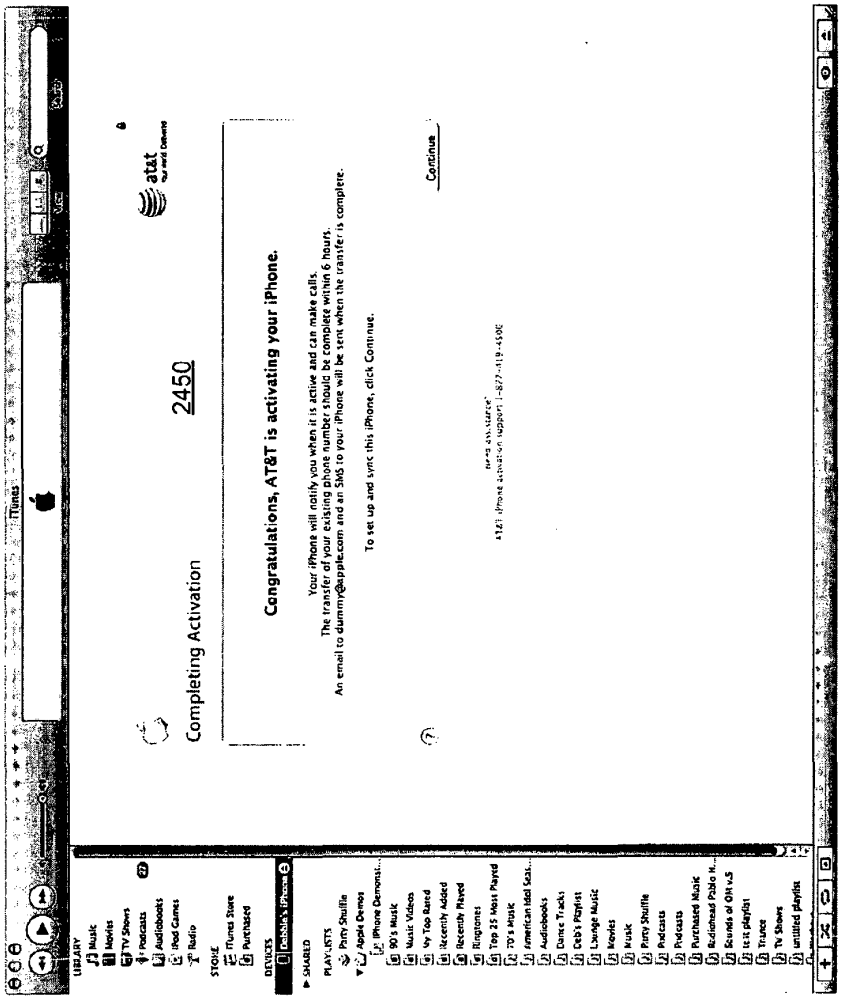


FIG. 24B

IPR2025-01572
Apple EX1002 Page 914

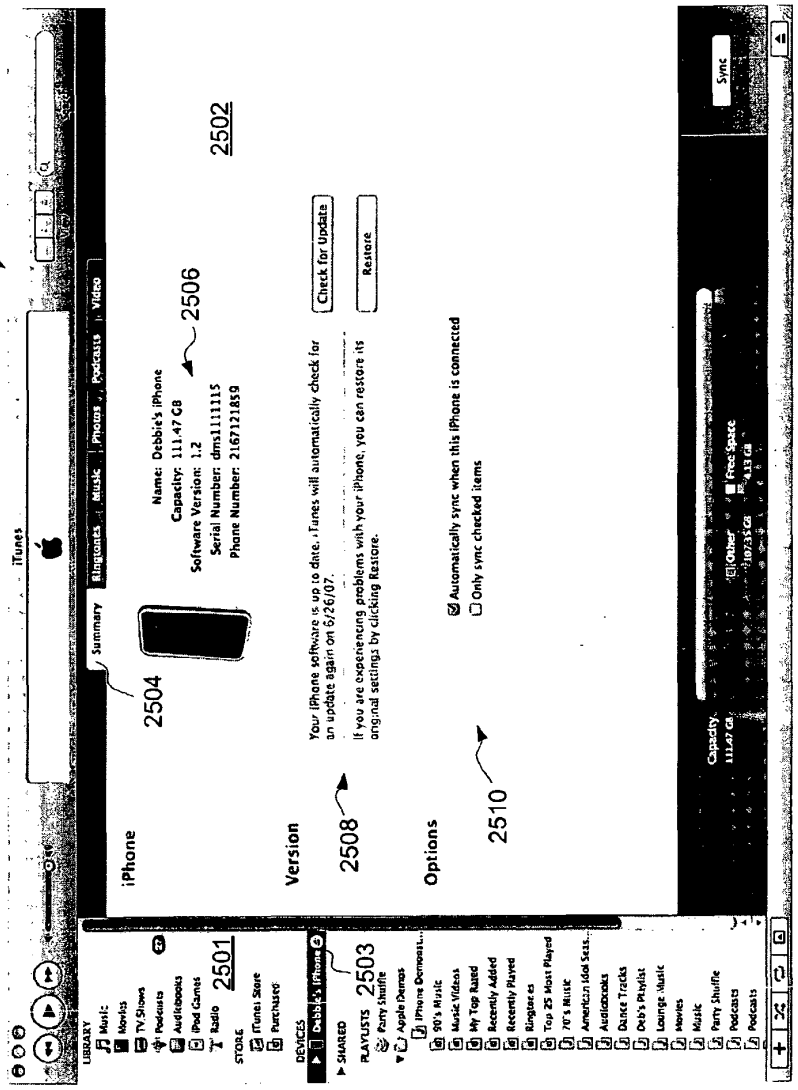


FIG. 25

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 915

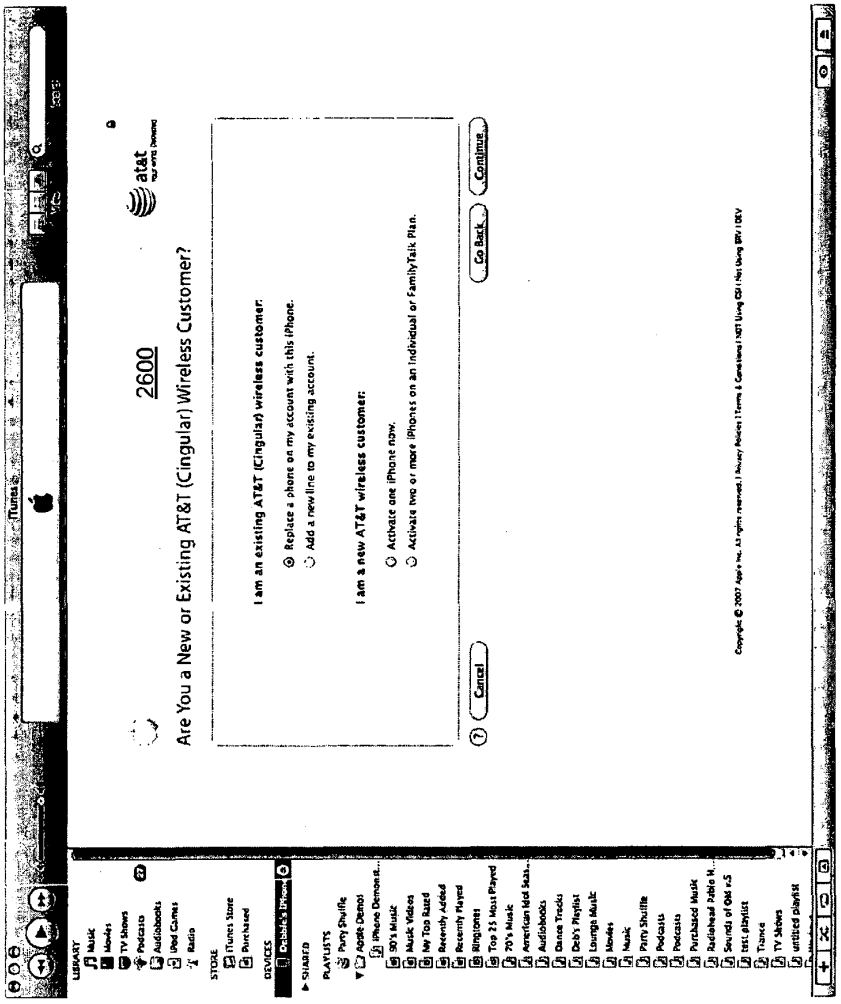


FIG. 26

IPR2025-01572
Apple EX1002 Page 916

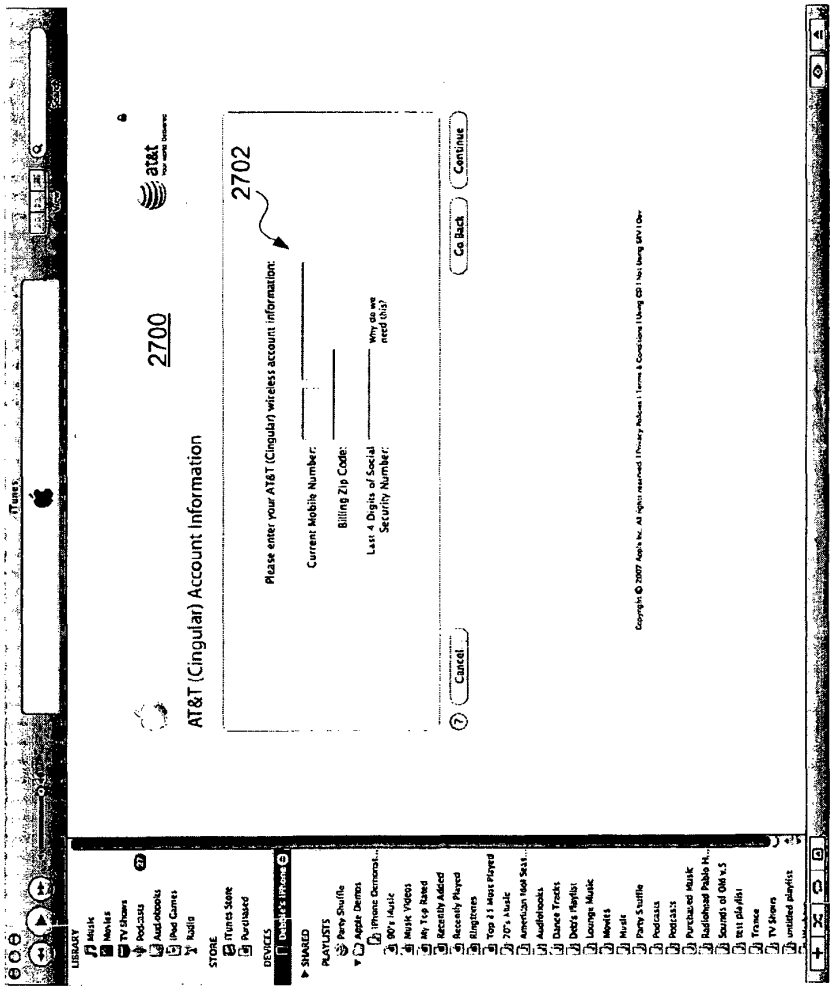


FIG. 27

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 917

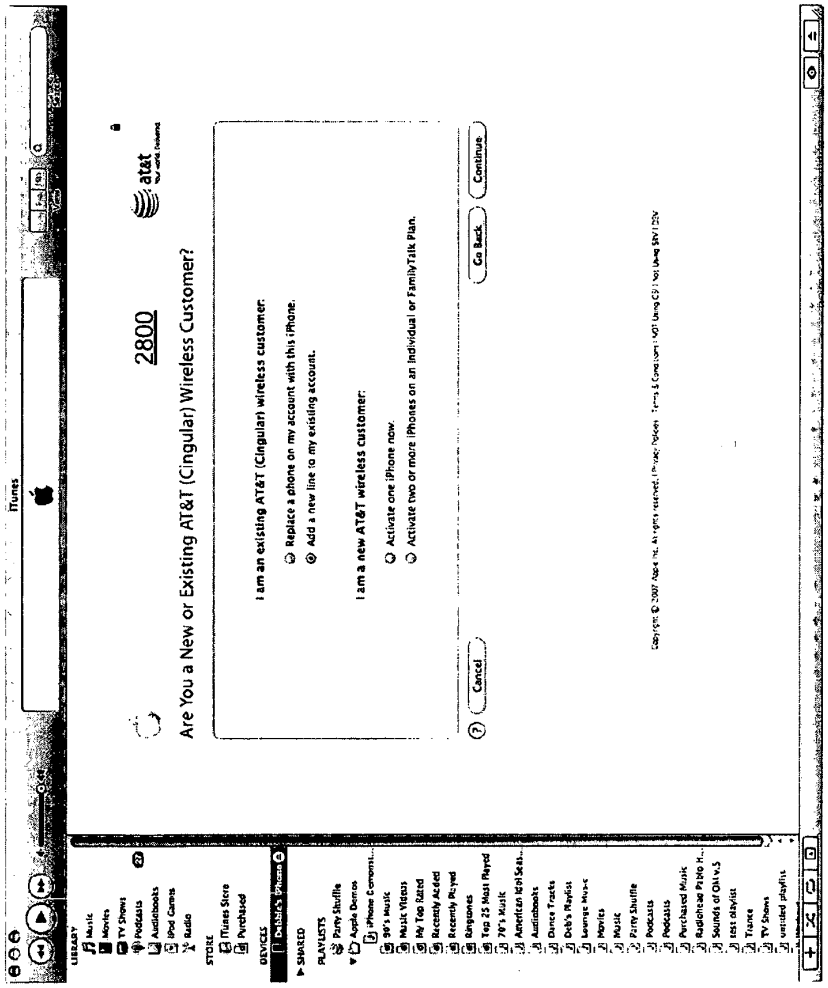


FIG. 28

IPR2025-01572
Apple EX1002 Page 918

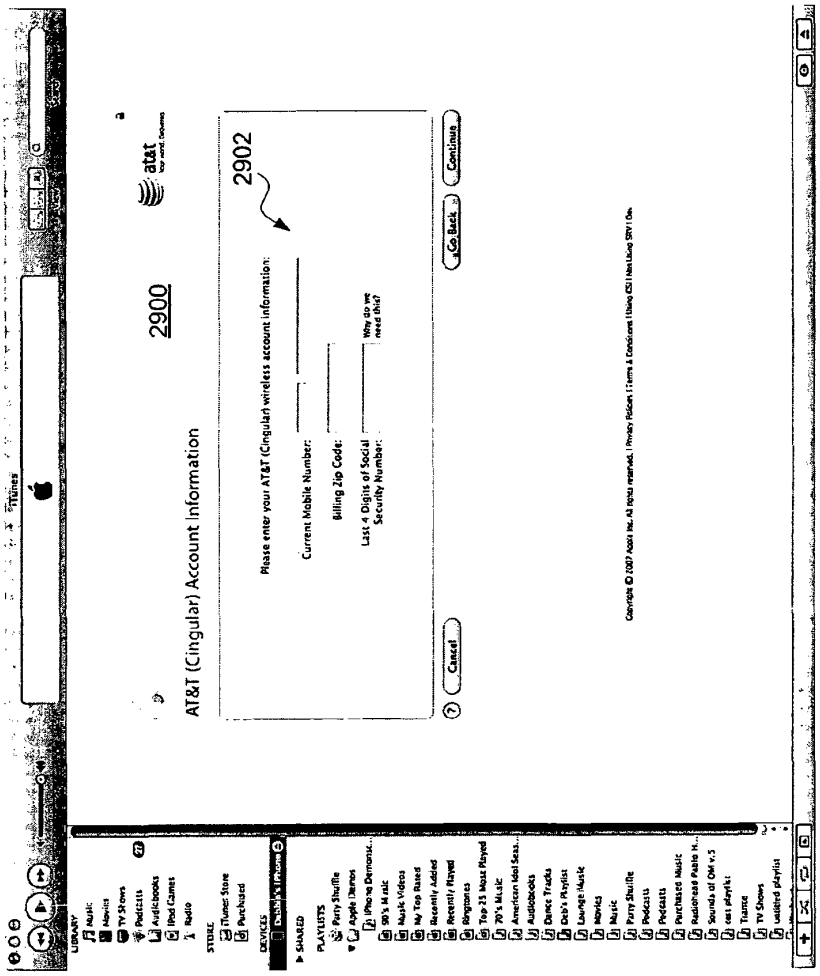


FIG. 29

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 919

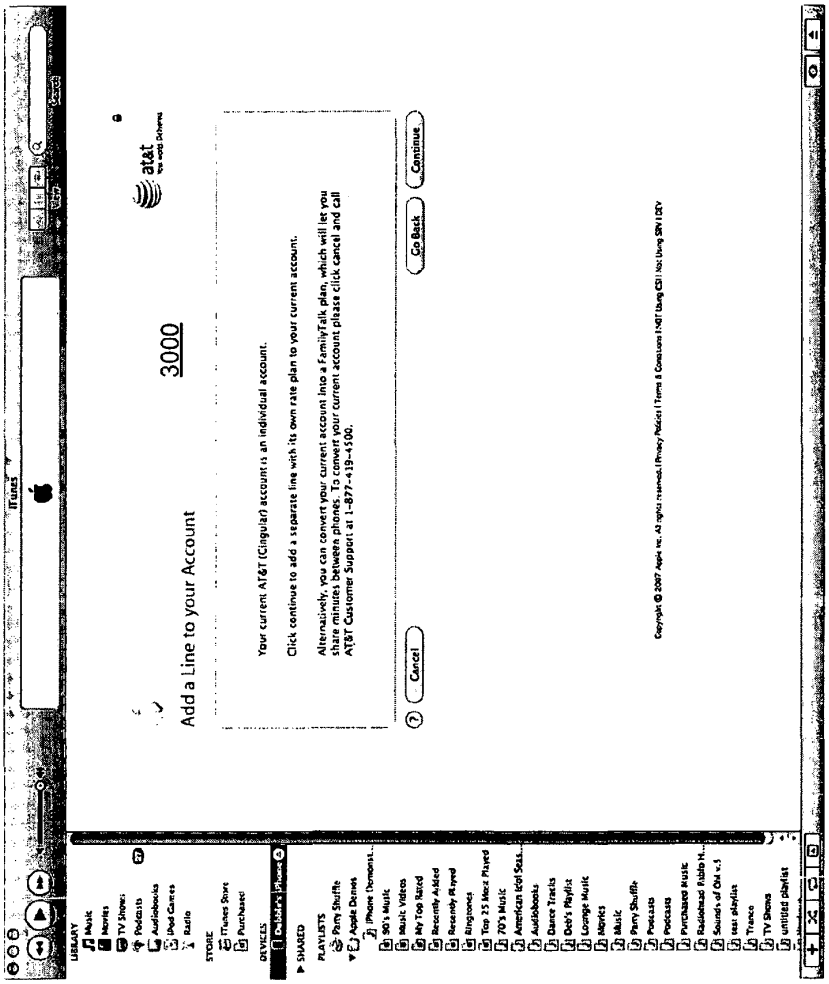


FIG. 30

IPR2025-01572
Apple EX1002 Page 920

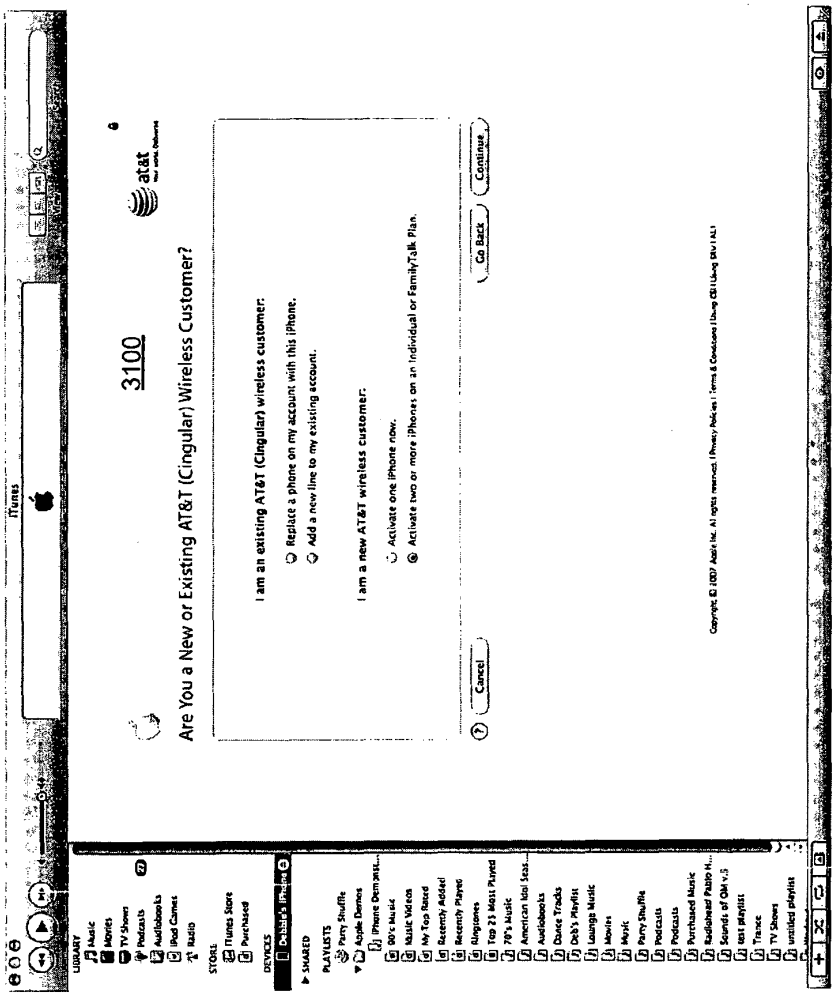


FIG. 31

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 921

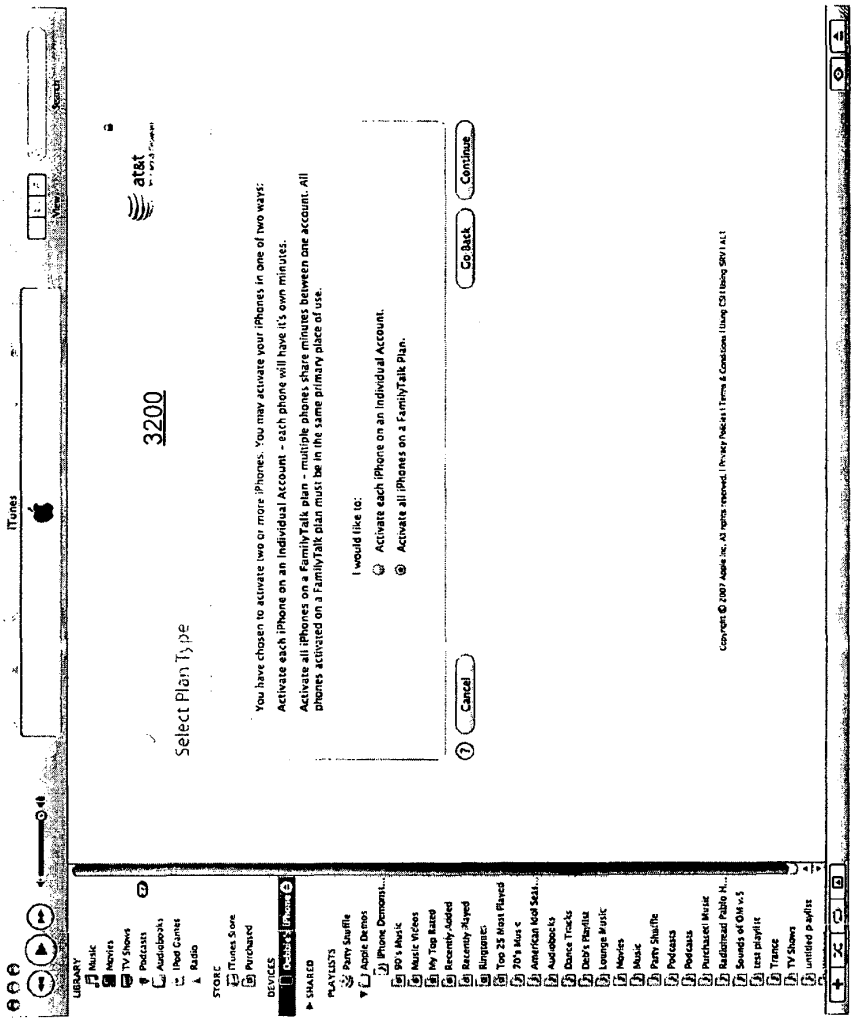


FIG. 32

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 922

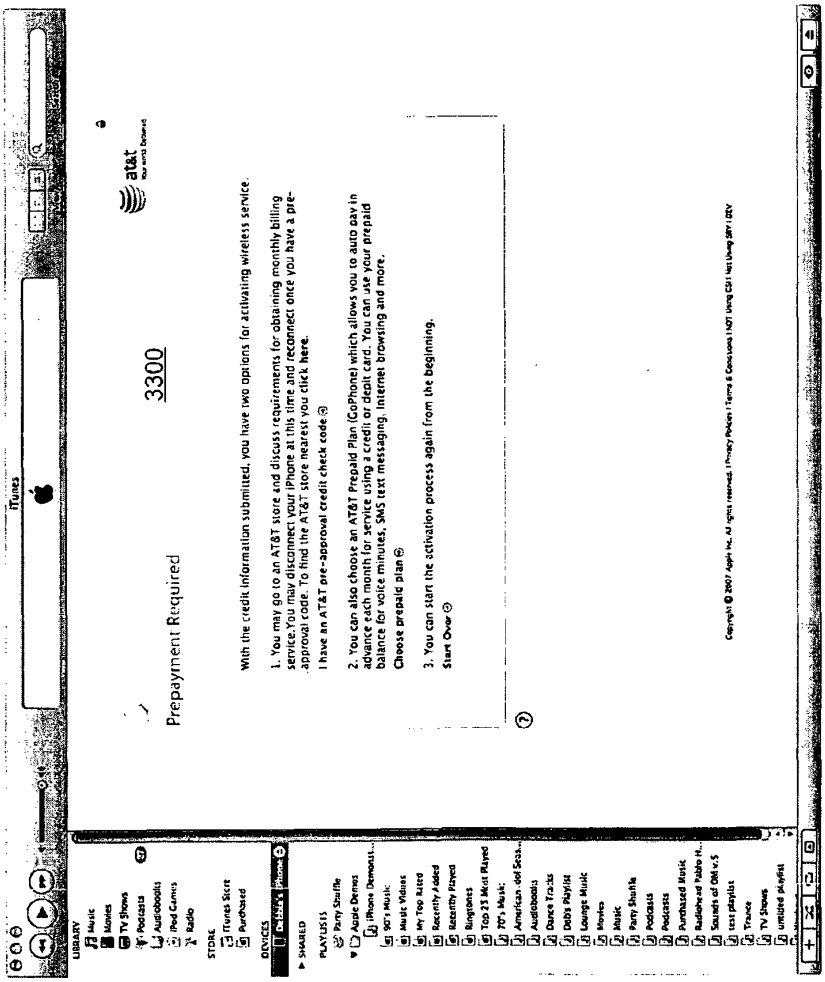


FIG. 33

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 923

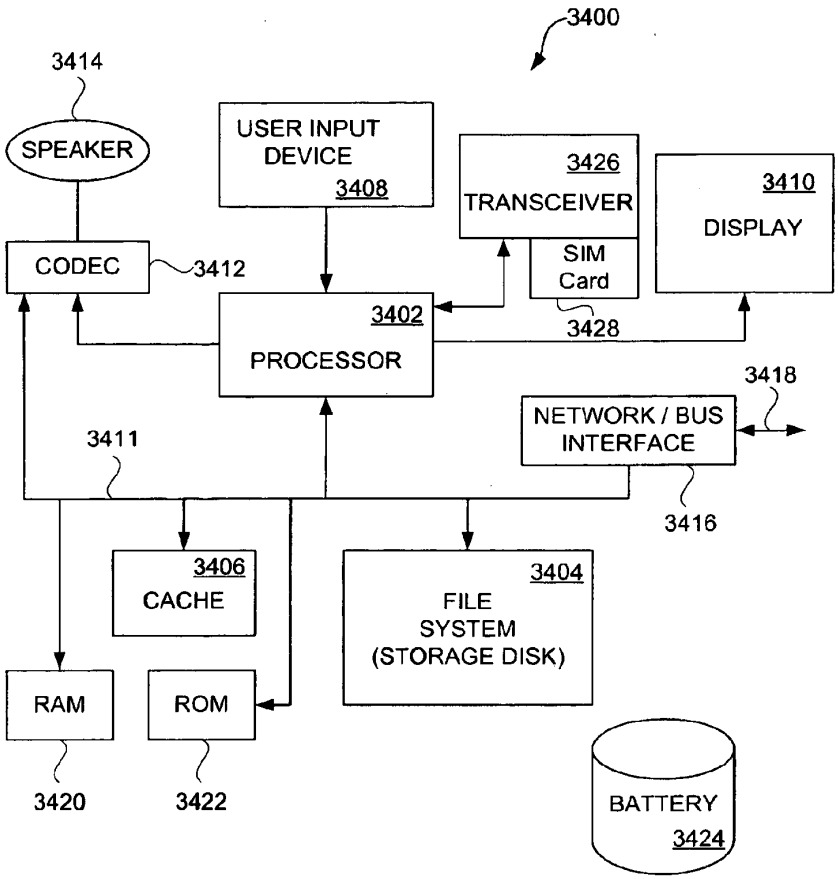


FIG. 34

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 924

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 08 25 0053

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2003/083068 A1 (WONG GREGORY A [US]) 1 May 2003 (2003-05-01) * paragraphs [0003] - [0007] * * paragraphs [0018] - [0023] * * figure 2 *	1-68	INV. H04Q7/38
X	US 2006/143098 A1 (LAZARIDIS MIHAL [CA]) 29 June 2006 (2006-06-29) * paragraph [0020] * * paragraph [0030] * * paragraphs [0049], [0050] * * paragraph [0060] * * paragraphs [0075], [0076] * * paragraphs [0087] - [0110] *	1-68	
X	US 2002/085530 A1 (TOYOSHIMA AKIHIKO [JP]) 4 July 2002 (2002-07-04) * paragraphs [0020] - [0022] *	1-68	
X	US 5 386 455 A (COOPER GERSHON N [US]) 31 January 1995 (1995-01-31) * column 1, line 38 - column 2, line 15 * * column 3, line 38 - column 5, line 49 * * figure 3 *	1-68	TECHNICAL FIELDS SEARCHED (IPC) H04Q H04M H04L
X	US 7 054 642 B1 (MATZ WILLIAM R [US] ET AL) 30 May 2006 (2006-05-30) * column 4, lines 39-52 *	1-68	
A	US 2004/235458 A1 (WALDEN CHARLES LEE [US] ET AL) 25 November 2004 (2004-11-25) * paragraphs [0005], [0006] * * paragraph [0011] * * paragraphs [0021] - [0023] * * claim 24 *	1-68	

-/--

4 The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	16 April 2008	Hegeman, Hans

CATEGORY OF CITED DOCUMENTS

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

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

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 925

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 08 25 0053

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	WO 01/15414 A (GTE LABORATORIES INC [US]) 1 March 2001 (2001-03-01) * the whole document *	1-68	
A	WO 03/041443 A (SIMPLE PRODUCTS INC [US]) 15 May 2003 (2003-05-15) * the whole document *	1-68	
A	US 2004/176133 A1 (LIPSIT JAMES MASON [US]) 9 September 2004 (2004-09-09) * the whole document *	1-68	
A	EP 0 367 361 A (GTE MOBILNET INC [US]) 9 May 1990 (1990-05-09) * the whole document *	1-68	
			TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	16 April 2008	Hegeman, Hans

CATEGORY OF CITED DOCUMENTS

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

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

EPO FORM 1503 03.82 (P04C01)

4

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 926

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 25 0053

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.

16-04-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003083068 A1	01-05-2003	US 2006142007 A1	29-06-2006
US 2006143098 A1	29-06-2006	NONE	
US 2002085530 A1	04-07-2002	NONE	
US 5386455 A	31-01-1995	NONE	
US 7054642 B1	30-05-2006	NONE	
US 2004235458 A1	25-11-2004	CA 2526680 A1 EP 1627539 A2 WO 2004107107 A2	09-12-2004 22-02-2006 09-12-2004
WO 0115414 A	01-03-2001	AU 6893900 A CA 2382298 A1 US 2001041591 A1	19-03-2001 01-03-2001 15-11-2001
WO 03041443 A	15-05-2003	US 2003092435 A1	15-05-2003
US 2004176133 A1	09-09-2004	NONE	
EP 0367361 A	09-05-1990	CA 2001857 A1 US 4958368 A	30-04-1990 18-09-1990

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 927

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

- US 76744707 A **[0088]**
- US 87931907 P **[0131]**
- US 67908207 A **[0131]**

BNSDOCID: <EP_____1942698A1_I_>

IPR2025-01572
Apple EX1002 Page 928

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 November 2010 (11.11.2010)

PCT

(10) International Publication Number
WO 2010/128391 A2

(51) International Patent Classification:
H04W 28/02 (2009.01)

(21) International Application Number:
PCT/IB2010/001084

(22) International Filing Date:
3 May 2010 (03.05.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/175,316 4 May 2009 (04.05.2009) US

(71) Applicant *(for all designated States except US)*: **BRIDGEWATER SYSTEMS CORP.** [CA/CA]; 303 Terry Fox Drive, Suite 500, Ottawa, Ontario K2K 3J1 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MOMTAHAN, Parham** [CA/CA]; 281 Lincoln Heights Road, Ottawa, Ontario K2B 5L7 (CA). **FREEN, Russ** [CA/CA]; 5 Clemow Avenue, Ottawa, Ontario, K1S 2A9 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, 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, KR, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: SYSTEM AND METHODS FOR MOBILE DEVICE-BASED DATA COMMUNICATIONS COST MONITORING AND CONTROL

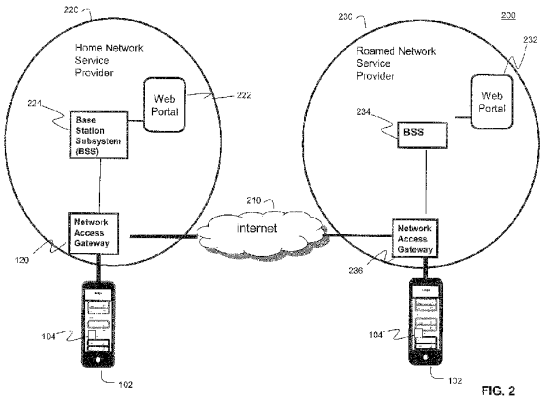


FIG. 2

(57) Abstract: Systems and methods for providing device-based data communications cost monitoring and controls are provided. In an embodiment, the method operates by receiving a registration request associated with a subscriber session, determining current data usage associated with the subscriber, and receiving data usage thresholds. The method further comprises receiving quotas associated with the subscriber session and collecting data usage information associated with the subscriber session. The method sends a notification to the subscriber when a predetermined quota is exceeded during the subscriber session and controls data usage. The system cost monitoring and control system comprises a usage policy server and a usage policy application. The usage policy application allows a subscriber to alter terms of a subscription. The usage policy application displays current data usage information on a per-network and per-application basis using subscriber profile information, subscriber session information, and prior subscriber usage history provided by the usage policy server.

WO 2010/128391 A2

IPR2025-01572
Apple EX1002 Page 929

System and Methods for Mobile Device-Based Data Communications Cost Monitoring and Control

FIELD OF THE INVENTION

[0001] The present invention relates generally to communications networks, more particularly, to monitoring and controlling data communications costs within wireless communications networks.

BACKGROUND

[0002] Portable computing devices such as laptop computers, personal data assistants (PDAs), smart phones and the like are in common usage, many featuring data communications support, powerful processors, larger and more colorful displays, and wireless networking and internet browsing capabilities. These advances in mobile technology have resulted in a dramatic increase in the volume of data communicated on wireless networks. These advances, coupled with subscribers seeking expanded mobility, will drive subscribers install and run data-hungry applications on their mobile devices. Data traffic is growing due to a combination of increasing market share of data-centric portable devices such as IPHONE™ and BLACKBERRY™ devices, lower wireless data subscription costs, higher wireless data throughput, and easier mobile access to data-intensive applications and rich content such as video. These trends are driving ever-increasing demands for wireless data communications.

[0003] Typically, users gain access to wireless data networks by purchasing a subscription plan from a service provider. In response to the explosive growth in mobile data traffic, service providers currently offer a wide variety of wireless subscription plan features such as actual usage plans, flat-rate plans, bandwidth caps that limit the amount of data per month for a mobile device, pre-paid and post-paid data plans. These plans typically impose limits on subscriber bandwidth consumption, often combined with additional fees for exceeding those limits. Bandwidth caps can alleviate network congestion by reducing overall mobile data traffic, but these caps reduce the attractiveness of data service for subscribers.

[0004] In a flat rate subscription plan a subscriber pays a fee for a billing cycle and is entitled to a set amount of network usage (i.e., a usage quota) during the billing cycle. For example, a subscriber may pay $30 for a month and be entitled to 500 minutes of network time. The usage quota can be specified as a time per billing cycle amount (e.g., 500 minutes per month) or as a data volume per billing cycle amount (e.g., 40 Mega Bytes per month). In some flat rate subscription plans, the usage quota is unlimited.

[0005] In an actual usage subscription plan a subscriber pays a set rate based on the actual amount of network usage during a billing cycle. For example, a user may pay $1 per minute of network usage. Actual usage plans can have incentives/penalties based on a subscriber's usage during a billing cycle. For example, in a subscription plan a subscriber may pay $1 per Mega Byte (MB) for the first 50 MBs and $2 per Mega Byte (MB) for every MB used beyond 50 MBs during the billing cycle. Subscription plans can combine aspects of flat rate plans and usage plans. For example, a subscriber may pay $30 per month for 40 MBs of wireless data usage and $1 per MB for every minute used after 40 MBs.

[0006] In the plans described above, as well as other subscriber plans, it is useful for a subscriber to be able to monitor his/her usage against one or more quotas.

[0007] Given the increasing versatility of mobile devices, it is helpful to implement a means by which these mobile devices can be used to monitor and control data communication costs, and to improve the subscriber experience.

[0008] Previous methods for network data communications cost monitoring and control are largely provider-centric, leaving the user with limited options to control and monitor costs. For example, a subscriber may be able to display cumulative consumption in MBs for the current month to determine if a monthly quota has been exceeded, but the subscriber cannot dynamically control and manage data communications costs without permanently changing his/her subscription plan. Provider-centric systems monitor usage and may allow subscribers to access usage information via a provider's web server, but they do not allow subscribers to set real time usage controls. For example, provider-centric systems do not allow subscribers to set data usage thresholds, quotas, or

caps on their devices each day based upon prior usage. Prior network data control techniques result in extra charges (i.e., due to roaming) and surprise data charges for subscribers who exceed bandwidth caps.

[0009] In prior systems, subscribers must rely on providers to monitor and control data usage. When a portable device moves to another provider network (i.e., roam), the amount of data usage information is limited to what the network the device is roaming in provides. For example, subscribers may not know what data charges (i.e., tariffs) apply while roaming. Prior techniques can result in excessive fees for subscribers who have unknowingly exceeded their plan's data quotas or caps. Subscribers cannot dynamically manage and control data costs for current data connections from their portable devices. In prior systems, subscribers only have data usage information in terms of overall volume of data used for all applications on a device, rather than the amount of data user per application. This lack of device-centric control and transparency limits the subscriber experience and causes subscribers to unnecessarily curtail their data usage.

[0010] What is therefore needed are systems and methods for providing device-based data communications cost monitoring and controls on a per application basis. What is further needed are systems and methods to allow subscribers to monitor and control expenditures on data services by providing proactive notification when subscribers are approaching bandwidth caps. What is also needed are systems and methods to allow subscribers to modify their plans either temporarily or permanently depending on their needs by providing add-on service availability (i.e., the ability to dynamically raise a bandwidth cap temporarily).

SUMMARY OF THE INVENTION

[0011] Embodiments of the present invention provide systems and methods that improve data communication usage and cost monitoring operations. An embodiment of the invention includes a system for monitoring and control of the

data usage that is based on a subscriber's device. Methods are disclosed that use a distributed system that runs on user equipment and mobile devices.

[0012] In an embodiment, a system provides subscribers with access to real-time information about data usage, and are given warnings to they are close to reaching bandwidth caps. The system notifies subscribers when they are close to reaching bandwidth caps or quotas and offers subscribers an opportunity to upgrade to a next service tier.

[0013] The invention also provides a method for managing data usage by allowing subscribers to gradually reduce download speeds, block some types of traffic, redirect device connection to on-portal applications, or select a new Quality of Service (QoS) level in order to manage bandwidth consumption. In this way, the invention makes different options available to subscribers, and lets them decide how to best-manage data usage according to their needs and priorities.

[0014] The invention additionally includes methods that use a distributed usage monitoring and control system that comprises applications that run on user devices.

[0015] Embodiments of the invention also include methods for performing cost monitoring and control on a per-application basis.

[0016] In an embodiment, the invention includes a centralized system for global monitoring and control of a plurality of mobile devices from a single, cross-provider (i.e., global) perspective.

[0017] Subscription data is used to calculate the likelihood of exceeding a quota (i.e., a quota breach) at a given time and this information is provided to a user of a mobile device. US Application No. 12/186,831, filed August 06, 2008 and entitled "Usage Measurement Collection and Analysis to Dynamically Regulate Customer Network Usage," describes methods and systems for calculating the likelihood of a quota breach. The present application includes the capabilities described therein. According to an embodiment of the present invention, a notification is sent to a subscriber when it is determined that a quota breach is likely to occur. In a related embodiment, subscribers are given the opportunity to

change a service tier associated with their subscription in order to prevent a likely quota breach.

[0018] In an embodiment, a service provider can present 'special offers' to a subscriber that provide the subscriber with an opportunity to change a service tier associated with their subscription. In further embodiments, acceptance of special offers can change service tiers associated with a subscriber's home network or roamed networks. According to embodiments of the invention, special offers can be sent to a subscriber by their home network service provider or roamed network service providers and are presented on the subscriber's mobile device.

[0019] In embodiments, both dynamic and static subscriber characteristics relative to a current usage session can be used to allow a subscriber to proactively manage data usage. Dynamic characteristics can be dynamic relative to the start of a usage session or relative to the usage session generally. An example of a dynamic characteristic relative to the start of a usage session is the type of data requested and the mobile applications requesting data. An example of a dynamic characteristic relative to the usage session is the total amount of data usage.

[0020] In a further embodiment, a subscriber characteristic used in data usage calculations includes knowledge of peak usage patterns (e.g., on peak/off-peak, weekdays).

[0021] It is an objective of the present invention that it may be incorporated into any mobile device capable of data communications.

[0022] In another embodiment, when a subscriber is roaming and the roaming traffic is not routed through the subscriber's home service provider home agent router or network access gateway, an interaction between the roamed service provider and home service provider occurs so that the home service provider has the information needed to control data usage in the roamed or visited network.

[0023] Another objective of the invention is to provide flexible policy descriptions for network service provider (carrier) charging plans. A further objective of the invention is to provide flexible tariff distribution. According to an embodiment of the invention, distribution of flexible policy descriptions associated to network service provider charging plans is achieved by using a

provider-based architecture. In an embodiment, a provider-dependent (i.e., carrier-based) architecture is also used to distribute tariffs associated with network service providers.

[0024] Further embodiments, features, and advantages of the invention, as well as the structure and operation of the various embodiments of the invention are described in detail below with reference to accompanying present drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] The accompanying drawings, which are incorporated herein and form a part of the specification, illustrate the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the pertinent art to make and use the invention.

[0026] FIG. 1 depicts an exemplary operating environment for providing network data communications cost monitoring and controls within a communications network, according to embodiments of the present invention.

[0027] FIG. 2 depicts an exemplary operating environment for providing data communications cost monitoring and controls in a roaming scenario including multiple communications networks, in accordance with an embodiment of the present invention.

[0028] FIG. 3 illustrates a provider independent system architecture for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention.

[0029] FIG. 4 illustrates a provider-based system architecture for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention.

[0030] FIG. 5 depicts an exemplary message flow diagram for a method providing data communications cost monitoring and controls when the provider-based architecture provided in FIG. 4 is used, according to an embodiment of the present invention.

[0031] FIG. 6 provides a method for monitoring and controlling data usage in accordance with the present invention.

[0032] FIGs. 7-11 depict a graphical user interface (GUI) for a mobile device to display data usage, edit usage limits, define tariffs, and accept offers to change service tiers, according to embodiments of the invention.

[0033] FIG. 12 depicts an exemplary computer system on which methods and systems herein may be implemented, according to embodiments of the present invention.

[0034] The present invention will now be described with reference to the accompanying drawings. In the drawings, like reference numbers can indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number may identify the drawing in which the reference number first appears.

DETAILED DESCRIPTION OF THE INVENTION

Mobile Environment

[0035] FIG. 1 provides an exemplary operating environment 100 for providing an adaptive window size for network data communications cost monitoring and controls, according to embodiments of the present invention. Operating environment 100 includes user equipment 102, network access gateway 120, optional service controller 130, policy controller 140, subscriber data repository 150, usage policy server 160, and application server farm 170. Operating environment 100 provides a simplified diagram of a communications network to illustrate the concepts of data communications cost monitoring and controls. As would be recognized by persons of skill in the art, embodiments of the present invention can be used in any type of communications network (e.g., wireline, wireless, or hybrid networks).

[0036] User equipment 102 is any device that provides a user access to one or more networks. User equipment 102 can include, but is not limited to, a

computer such as user equipment 102a, a personal digital assistant (PDA) such as user equipment 102b, a wireless phone such as user equipment 102c, a smart phone, other wireless mobile devices, and/or wired communications devices.

[0037] Access network 110 is a communications network that couples user equipment 102 to a packet data network (not shown). Access network 110 may be a third generation partnership project (3GPP) access network or a non-3GPP access network. Exemplary 3GPP access networks include the UMTS terrestrial radio access network (UTRAN) and the GSM EDGE radio access network (RAN). Other access networks include, but are not limited to, WiFi, WiMAX, CDMA2000, GSM, and UMTS.

[0038] Network access gateway 120 provides an interface between access network 110 and a packet data network (not shown). In a 3GPP network, network access gateway 120 may be the Gateway General Packet Radio Service (GPRS) Support Node (GGSN). Note that network access gateway 120 may also act as a policy enforcement point.

[0039] Policy controller 140, at a high level, includes subscriber profiles and network policies needed to manage network resources, such as bandwidth, according to a subscriber, session, and/or application. A service provider may apply a policy based on business rules associated with a variety of factors (e.g., service tiers and/or dynamic parameters such as time of day).

[0040] Policy controller 140 includes a policy and charging rules function (PCRF) 142 and a quota manager 144. For example, in a 3GPP network, PCRF 142 acts as a decision point for policy and charging control of service data flows. PCRF 142 is configured to select and provide the applicable policy and charging control decisions to the policy control enforcement point.

[0041] Usage policy server 160 works in conjunction with policy controller 140 to extend policy and charging control of service data flows to user equipment 102. These data flows may be monitored and controlled on a per subscriber, per user equipment, or per application basis. For example, control and metering of data flows from applications hosted in application server farm 170 to user equipment 102a may be performed by usage policy server 160. Alternatively,

control and metering of data flows for a particular subscriber using user equipment 102a may be performed by usage policy server without regard to the applications being invoked by the subscriber. Similarly, control and metering of data flows between a pool of related subscribers (i.e., subscribers in the same family, organization, or corporation) using user equipment 102a-c may be performed by usage policy sever 160, regardless of the applications involved in the data flows. Although the exemplary environment 200 depicts usage policy server 160 as a separate server from policy controller 140, as would be understood by those skilled in the relevant art(s) usage policy server 160 may be implemented as software residing in policy controller 140. Conversely, policy controller 140 may comprise software residing on usage policy server 160

[0042] According to an embodiment of the invention, a subscriber using user equipment 102 can set usage limits in mobile usage policy application 104 running on user equipment 102. For example, a subscriber using user equipment 102a can use mobile policy application 104a to set total daily usage limits in Mega Bytes (MBs), which are communicated to usage policy server 160 via access network 110, network access gateway 120, and policy controller 140. Subscribers can also set data usage notification and stop thresholds in mobile usage policy application 104. Upon reaching a notification threshold (i.e., 400 MBs in the example embodiment depicted in FIG. 7), a subscriber will receive a notification on user equipment 102. At that point, the subscriber can optionally can set a new, higher usage limit in mobile usage policy application 104, or choose to curtail data usage. Upon reaching a stop threshold (i.e., 600 MBs in the example embodiment depicted in FIG. 7), a subscriber will be unable to use additional data services on user equipment 102 until a higher usage limit is set in mobile usage policy application 104 or server-side usage policy application 164.

[0043] Usage policy server 160 provides usage policy data to policy controller 140. Quota manager 144 is configured to collect data communications usage and cost data. Quota manager 144 provides data communications cost monitoring and data to user equipment 102a-c via network access gateway 120 and access network 110. If the subscriber exceeds a data usage cap or threshold, quota

manager 144 provides this information to user equipment 102a-c and usage policy server 160. In an embodiment, server-side usage policy application 164 running on usage policy server 160 allows subscribers to set data usage controls via a web portal (See FIGs. 2 and 3). Data usage controls include, but are not limited to, total daily usage thresholds, total hourly usage thresholds, per-application usage thresholds, per-device usage thresholds, and thresholds based on data sources (i.e., Uniform Resource Locator/URL addresses or Internet Protocol/IP addresses). In an alternative embodiment, a mobile usage policy application 104 running on user equipment 102 allows subscribers using user equipment 102 to set data usage controls, such as, but not limited to the thresholds mentioned above directly on user equipment 102.

[0044] Quota manager 144 is configured to set adaptive fair usage windows according to a variety of techniques including, but not limited to, using pre-defined value or values, calculating windows based on one or more formulas, and/or determining window based on how quickly previous windows were violated. These techniques are described in further detail in US Application No. 61/153,910, filed February 19, 2009, and entitled "Adaptive Window Size for Network Fair Usage Controls." The capabilities described therein are included in the current application.

[0045] Policy controller 140 is coupled to subscriber data repository 150. Subscriber data repository 150 includes a subscriber profile database 152, a subscriber state database 154, and a subscriber usage database 156. Although depicted as three separate databases in FIG. 1, a person of ordinary skill in the art will recognize that subscriber profile, subscriber state, and subscriber usage data may be stored in any number of databases.

[0046] Policy controller 140 is further coupled to network access gateway 120. In an embodiment, the interface between policy controller 140 and network access gateway 120 is a Gy interface.

[0047] Subscriber state database 154 includes information that identifies and defines a subscriber's network session. Subscriber state information includes the subscriber identifier for the session. In embodiments of the invention, subscriber

identifiers may be one or more of a Mobile Subscriber ISDN Number (MSISDN), a Mobile Identification Number (MIN), a Private Identifier, information about the network such as the IP address the subscriber is currently using and what network or networks to which the subscriber is currently connected, device information such as the device being used and the version of the software, location and roaming information, and other unique state information.

[0048] When a subscriber connects to any network, the core elements of the network assign an Internet Protocol (IP) address to the subscriber. At that time, the subscriber session begins and subscriber state information is created, derived and captured. For example, state information is typically generated either through RADIUS accounting or through interactions with the dynamic host control protocol (DHCP) service on a network. The accounting message feeds are generated to a Remote Authentication Dial In User Service (RADIUS) engine or an authentication, authorization and accounting (AAA) service from core network elements.

[0049] Subscriber profile database 152 includes static information about the subscriber. This information may include the service tier (e.g., gold, silver, bronze) assigned to the subscriber. In an embodiment of the invention, service tiers are associated with Quality of Service (QoS) levels.

[0050] Subscriber usage database 156 includes static and dynamic information related to the subscriber's history. The subscriber's history includes, but is not limited to the subscriber's data usage history. In embodiments of the present invention, subscriber usage database 156 may store information about the amount of data used on a per-application basis by the subscriber's user equipment 102 in previous sessions. Usage policy server 160 uses the per-application usage data from prior sessions to inform the subscriber about which applications running on user equipment 102 have consumed the most bandwidth or data based on previous behavior patterns.

[0051] According to an embodiment of the invention, a carrier or provider-based infrastructure is used wherein the service provider infrastructure provides data metering and control. In this architecture, usage policy server and server-side

usage policy application 164 are used to control and meter data usage on user equipment 102.

[0052] In another embodiment, a carrier-independent is used whereby metering and control is performed on user equipment 102 using mobile usage policy application 104. In this embodiment, some centralized functions are performed by policy controller 140 and usage policy server 160, such as controlling data usage policies across multiple user equipment 102a-c. In this embodiment, longer-term historical storage of usage information occurs in subscriber usage database 156 within subscriber data repository 150.

[0053] In an embodiment, a hybrid architecture gathers usage data on user equipment 102 but long-term storage of the usage data occurs in subscriber usage database 156 within subscriber data repository 150. In this way, centralization is performed within a service provider infrastructure. This architecture is useful for the roaming scenario depicted in FIG. 2 and described below.

[0054] FIG. 2 depicts an exemplary operating environment 200 for providing data communications cost monitoring and controls while roaming. Although the exemplary environment 200 depicts two network service providers, home network service provider 220 and roamed network service provider 230, as would be understood by those skilled in the relevant art(s), user equipment 102 may connect to a plurality of roamed network service providers 230 while roaming.

[0055] FIG. 2 is described with continued reference to the operating environment of FIG. 1. However, environment 200 is not limited to that embodiment.

[0056] Mobile data costs for a subscriber using user equipment 102 may be based on data volume used within a period. For example, a subscriber's subscription may entail a charge of $60 up to a 1Giga Byte (GB) cap of data access each month with a $3 per MB charge after the 1GB cap has been exceeded. Data costs also vary based on the home network service provider 220 that user equipment 102 is homed in or connected to. Typically, data costs increase when user equipment 102 is roaming in roamed network service provider 230. Due to these and other dynamic factors that can increase data costs, embodiments of the

present invention enable subscribers to monitor and control expenditure on data services on user equipment 102 on a real time basis.

[0057] In accordance with a 'provider-centric' embodiment of the invention, monitoring and control of usage and charging for data is performed by methods and systems that reside within home network service provider 220 and remain under the control of home network service provider 220. In the provider-centric embodiment, home network access gateway 120 and roamed network access gateway 236 monitor and control packet traffic between user equipment 102 and the Internet 210. Home network access gateway 120 and roamed network access gateway 236 generate usage accounting records that are input to off-line or on-line (prepaid) billing and reporting systems residing in base station subsystems 224 and 234. Examples of home network access gateway 120 and roamed network access gateway 236 include, but are not limited to gateway GPRS Support Node (GGSN), Packet Data Serving Node (PDSN), Deep Packet Inspection (DPI), and "Evolved NodeB (eNodeB).

[0058] Home network service provider 220 and roamed network service provider 230 may provide visibility of data usage records via a website user interface to subscribers that log in to check their account via web portals 222 and 232.

[0059] According to an embodiment, subscribers can monitor and control their data usage via web portals 222 and 232. For example, subscribers can select service extensions, data usage boosts, a lower bandwidth service, or other alternatives via home network web portal 222 and/or roamed network web portal 232. These changes are then passed to usage policy server 160 and propagated to server-side usage policy application 164. In an alternative embodiment, changes made via home network web portal 222 and roamed network web portal 232 are propagated to mobile usage policy application 104 resident on user equipment 102.

[0060] In another embodiment, when a subscriber is roaming and the roaming traffic is not routed through the subscriber's home service network provider 220 home agent or home network access gateway 120, an interaction between a usage policy server 160 in roamed network service provider 230 and a usage policy

server 160 in home network service provider 220 is initiated. This interaction between the respective usage policy servers includes a request being sent from usage policy server 160 in home network service provider 220 to a usage policy server 160 in roamed network service provider 230. According to an embodiment, the request is for information that home network service provider 220 needs in order to affect data usage controls for user equipment 102 while it is accessing data in roamed network service provider 230.

[0061] In an embodiment, to prevent unexpectedly high roaming charges from roamed network service provider 230, a subscriber using user equipment 102 may select, using usage policy application 104 to be barred from all or some data applications while roaming in the network of roamed network service provider 230. For instance, a subscriber using a mobile device such as user equipment 102 may wish to avoid the high cost of data services while they are outside the coverage area of home network service provider 220, but retain the data service when they are not roaming.

[0062] According to an embodiment, while user equipment 102 is using roamed network service provider 230, a subscriber may opt to have certain applications from application server farm 170 blocked.

[0063] Operators of home network service provider 220 and roamed network service provider 230 can detect access to on- or off-portal applications, and they typically choose to charge less, or impose no data fees, for access to on-portal applications from user equipment 102. In an embodiment, a subscriber may choose to select only on-portal applications (either in home network service provider 220 or roamed network service provider 230) in order to reduce data usage and costs.

[0064] In instances when access network 110 depicted in FIG. 1 becomes congested, an embodiment of the invention provides real-time traffic information from access network 110 and, more specifically, from individual base station subsystems 224 and 234 which enables operators of home network service provider 220 or roamed network service provider 230 to identify areas of congestion within their respective access networks 110. Policy controller 140

includes operator tools to contain congestion in real-time by temporarily enforcing more stringent policies (i.e., not allowing bursting behavior, or assigning lower priority to subscribers with low-tier service plans).

[0065] In an embodiment, in order to prevent 'bill shock' due to exceeding data quotas and in order to extend usage control to subscribers, mobile usage policy application 104 works in conjunction with policy controller 140 to provide proactive notifications to user equipment 102 when subscribers are nearing bandwidth usage thresholds or data roaming charge limits in roamed network service provider 230. Subscribers can then be given choices in real-time in mobile usage policy application 104, such as a service extension, a data usage boost, a lower bandwidth service, or other alternatives. In addition, operators of home network service provider 220 or roamed network service provider 230 can extend control to subscribers to set personalized usage caps that can be updated in real-time based on personal financial limits, or to boost roaming data usage while a subscriber is traveling.

Data Monitoring and Control Systems

[0066] FIG. 3 illustrates an architecture for a system 300 for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention. System 300 is provider independent in that the architecture is distributed between user equipment 102 and a usage policy server 160.

[0067] FIG. 3 is described with continued reference to the operating environments of FIGs. 1 and 2. However, system 300 is not limited to those embodiments.

[0068] In an embodiment, monitoring and control of the data usage is based on user equipment 102 using mobile usage policy application 104, instead of within the infrastructure of home network service provider 220 or roamed network service providers 230. This distributed system runs on user equipment 102 and usage policy server 160. In system 300, the charging/cost monitoring and control

can be performed down to the level of the individual applications 306 running on user equipment 102. Applications 306 may include, but are not limited to games, social networking applications, Voice over Internet Protocol (VOIP) applications such as Skype, and wireless access to data-intensive web sites that host multimedia content such as video.

[0069] According to an embodiment, a device usage control subsystem (executes on user equipment 102 and monitors data flows (denoted as 1-4) on user equipment 102. The device usage control subsystem comprises the following components: local store 308, application controller 310, and mobile usage policy application 104. These components are described in the following paragraphs.

[0070] Application controller 310 is installed to mediate between applications 306 and communication stack 312 of user equipment 102. In an embodiment, communication stack 312 is a Transmission Control Protocol (TCP)/Internet Protocol (TCP/IP) stack. Application controller 310 presents a virtual socket layer to applications 306. Application controller 310 also counts how many bytes each application 306 sends and receives (denoted as data flow 1). Application controller 310 also stores the data usage on a per-application basis in local store 308 (denoted as data flow 4). Application controller 310 checks for application data usage threshold limits defined in the local store by the mobile usage policy application 104. In an alternative embodiment, application controller 310 checks for application data usage threshold limits defined in the global store 368 by the server-side usage policy application 164, which can be accessed via calls to Application Programming Interface (API) 366.

[0071] In an embodiment, data usage information for a single device is stored in a data store, such as local store 308 on user equipment 102. 2. Local store 308 may use non-volatile storage on user equipment 102 to hold information such as, but not limited to, data usage for each application 306, data budgets, thresholds, tariff information, and statistics regarding highest budget applications 306. Each of these types of information is described below.

[0072] Each of the types of information described below may optionally be stored in local store 308 on user equipment 102. The information described

below may also be periodically imported from or exported information to global store 368 residing on one or more usage policy servers 160.

[0073] Data 'budgets' for applications 306 or groups of applications 306 can be set in mobile usage policy application 104 or server-side usage policy application 164. In an embodiment, after reaching its budgeted allocation for a given period, an application 306 is capped or blocked from further data network usage. According to this embodiment until that period is elapsed (or the budget is changed or over-ridden by a subscriber), application 306 will be blocked from performing additional data transactions, thereby allowing the subscriber to control data costs that may otherwise cause 'bill shock.'

[0074] Thresholds for applications 306 are kept, whereby the subscriber is notified that an application 306 or group of applications 306, if a subscriber has set a threshold of 75% for an application 306, when that application 306 has consumed 75% of its data budget, the subscriber will receive a notification at user equipment 102.

[0075] Tariffs comprise information kept for each known potential roamed network service provider 230 in which the subscriber can roam, so that the user has control over which roamed network service provider 230 would be most cost-effective to use. Tariff information pertaining to a plurality of roamed network service providers 230 may be stored in a local store 308 on user equipment 102. Tariff data for each roamed network service provider 230 may reside in a database or data store on usage policy server 160, such as global store 368.

[0076] According to an embodiment, local store 308 may periodically import or export tariff information via data flows 5 and 6, respectively, to global store 368 residing on one or more usage policy servers 160 associated with one or more roamed network service providers 230. Tariff information stored in global store 368 and a plurality of local stores 308 can be used to provide flexible tariff distribution. In an embodiment of the invention, a carrier-based architecture is used to distribute tariffs stored in global store 368 and local stores 308.

[0077] Statistics regarding highest budget applications 306 include cumulative data usage information kept in order to meter and display subscribers, user

equipment 102, and/or applications 306 using highest budgeted amount of data for a give period. For example, statistics may be kept on a single user equipment 102 regarding applications 306 on a particular user equipment 102 which have used the largest amount of data. Statistics may also be compiled on usage policy server 160 regarding data usage for a plurality of subscribers and/or user equipment 102.

[0078] In accordance with an embodiment of the invention, data usage pertaining to a plurality of subscribers is stored in a data store on usage policy server 160, such as global store 368. According to an embodiment, local store 308 may periodically import or export information via data flows 5 and 6, respectively, to global store 368 residing on one or more usage policy servers 160 associated with one or more network service providers.

[0079] According to an embodiment, the types of data described in the following paragraphs are modeled by usage policy application 104 and stored in a local store such as local store 308.

[0080] Usage entity data, including, but not limited to data identifying a network service provider such as home network service provider 220, network type (WiFi, 3G, etc.), user equipment 102 device type, device group, subscriber or user, user group, application 306, and groups of applications 306 may be stored in local store 308.

[0081] Quota information, such as a quota expressed in MBs or GBs and cost for additional quota levels, may be modeled by usage policy application 104 and stored in a local store such as local store 308. Quotas may be modeled and stored on the network service provider level, subscriber level, subscriber group level, for each application 306, and for groups of applications 306.

[0082] Threshold information such as the percentage of a quota reached in a period (i.e., monthly, weekly, and/or daily) may also be stored in local store 308. Thresholds may be modeled and stored on the network service provider level, subscriber level, subscriber group level, for each application 306, and for groups of applications 306.

[0083] Information regarding data costs incurred may also be modeled by usage policy application 104 and stored in a local store such as local store 308. Data costs may be modeled and stored on the network service provider level, subscriber level, subscriber group level, for each application 306, and for groups of applications 306.

[0084] Usage intervals may be stored be stored in local store 308 on a daily, weekly, and monthly basis. Usage intervals pertaining to a plurality of subscribers and user equipment 102 may also be stored in global store 368.

[0085] Tariff information for a plurality of networks regarding data prices (i.e., expressed as cost per Byte, MB, or GB) may also be stored in a local store such as local store 308. Tariff information is collected and stored on a network level.

Mobile Usage Policy Application

[0086] With continued reference to FIG. 3, in an embodiment, mobile usage policy application 104 provides the functionality described in the following paragraphs.

[0087] Mobile usage policy application 104 provides a user interface for monitoring and control (denoted as data flow 3). An exemplary user interface is provided in FIGs. 7-11, which are described in detail below.

[0088] Mobile usage policy application 104 also defines the data and policies that application controller 310 and local store 308 require (denoted as data flow 2 in FIG. 3).

[0089] The following are the types of data usage policies defined by mobile usage policy application 104 for application controller 310 on user equipment 102.

[0090] Mobile usage policy application 104 can set data usage quotas, thresholds (including alert and stop thresholds), allowable maximum tariffs (i.e., tariff limits expressed in terms of maximum acceptable costs per Byte, MB, or GB), allowable network service providers (i.e., allowed roamed network service providers 230 for a given subscriber, user equipment 102 and/or application 306),

IPR2025-01572
Apple EX1002 Page 948

and allowable network tariff minimums. For example, mobile usage policy application 104 may only allow a given subscriber, user equipment 102, or application 306 to access a roamed network service provider 230 tariff less than a certain currency amount per storage unit (i.e., US dollars per MB or GB).

Usage Policy Server and Server Side Usage Policy Application

[0091] In an embodiment, usage policy server 160 hosts server side usage policy application 164, global store 368, a Global Policy Controller, and web portal 222.

[0092] Global store 368 optionally collects data usage information from local stores 308 from a plurality of user equipment 102. In an embodiment, global store 368 comprises a database that provides rolled up, or per user equipment 102, per-subscriber, per-application 306 breakdowns, or views of usage data within various contexts. These contexts may include, but are not limited to, corporations, organizations (i.e., departments), and a subscriber. The level of granularity of data stored in global store 368 allows subscribers and network administrators to run data queries and generate reports regarding data usage for a single subscriber, single user equipment 102, groups of subscribers, and related sets of user equipment 102 (i.e., user equipment leased by an organization or corporations) for a given period. In an embodiment, these queries and reports can be accessed via web portal 222.

[0093] Global store 368 on usage policy server 160 optionally stores and distributes the per user equipment 102 information. In this way, usage policy server 160 can be used to provide centralized provisioning of user equipment 102.

[0094] Global policy controller 370 is an application on usage policy server 160 that enables access to global store 368 and drives global store 368 to collect information from a plurality of user equipment 102 (denoted as data flow 5). Global policy controller 370 also drives global store 368 to provision information to a plurality of user equipment 102 (denoted as data flow 5).

Provider Based System

[0095] FIG. 4 illustrates an architecture for a provider-based system 400 for providing data communications cost monitoring and controls within a communications network, in accordance with an embodiment of the present invention.

[0096] FIG. 4 is described with continued reference to FIGs. 1-3. However, system 400 is not limited to those embodiments.

[0097] In the embodiment of system 400, the infrastructure of a network service provider provides data usage metering and control. Usage policy server 160 provides interface 404 to subscribers using user equipment 102 to allow subscribers to monitor and control charging for data usage.

[0098] In an embodiment the data usage metering and control is web based and accessed via web portal 222. Alternatively, data usage metering and control is device application based using interface 404 invoked locally on user equipment 102. Interface 404 allows the device to register with usage policy server 160 (denoted as data flow 1). After registration, user equipment 102 is synchronized with usage policy server 160 and local store 308 is updated (denoted as data flow 2).

[0099] Usage policy server 160 also allows subscribers and network administrators to access web interface via web portal 222 to fetch values for data usage attributes (denoted as data flow 3) such as, but not limited to thresholds and quotas on a per application 306, home network service provider 220, roamed network service provider 230, or subscriber basis.

[0100] Usage policy server 160 also stores usage data for all registered user equipment 102 in subscriber usage database 156 for a given period (e.g., 2 months).

[0101] Usage policy server 160 then registers with online and offline charging systems such as policy and charging rules function (PCRF) 142. In embodiments, the charging systems may include AAA and other protocols, capable of receiving data usage information for user equipment 102.

IPR2025-01572
Apple EX1002 Page 950

[0102] According to an embodiment, PCRF 142 receives a bulk registration request from usage policy server 160 (denoted as data flow 4). The bulk registration request comprises data usage information for a plurality of user equipment 102 that has registered with usage policy server 160. The data usage information contains threshold and stoppage policies based on criteria such as data volume and the characteristics of roamed network service provider 230.

[0103] System 400 can be used to provide flexible policy descriptions for a network service provider's charging plan. For example, a network service provider can furnish its policy and charging rules from PCRF 142 via usage policy server 160. The provider-based architecture illustrated in FIG. 4 enables distribution of flexible policy descriptions corresponding to network service provider charging plans via data flows between PCRF 142 and usage policy server 160.

[0104] System 400 and the provider-based architecture depicted in FIG. 4 can also be used to provide flexible tariff distribution. Tariffs comprise information kept for each known potential roamed network service provider 230 in which a subscriber can roam. Access to this information on user equipment 102 is useful when a subscriber wants to determine which potential roamed network service provider 230 will be most cost-effective to use. Tariff information pertaining to a plurality of roamed network service providers 230 may reside in a database or data store on usage policy server 160 to be distributed to a plurality of user equipment 102.

[0105] PCRF 142 accesses usage information forwarded by one or more network access gateways 120. In an embodiment, this usage information is received by network access gateway 120 via a radio access network (RAN) 406. PCRF 142 sends usage stream information comprising current data usage information for user equipment 102 to usage policy server 160 (denoted as data flow 5).

[0106] Usage policy server 160 requests that PCRF 142 control usage (i.e., affect bearer channel) for user equipment 102 once a stoppage decision is made by PCRF 142 (denoted as data flow 6).

Data Monitoring and Control Methods

[0107] FIG. 5 depicts an exemplary message flow diagram for a method 500 for providing data communications cost monitoring and controls when the provider-based architecture provided in FIG. 4 is used, according to an embodiment of the present invention. FIG. 5 is described with continued reference to FIG. 4. However, method 500 is not limited to that embodiment.

[0108] In step 505, a subscriber, using interface 404 on user equipment 102 enters data needed to make an initial request to register user equipment 102. In another embodiment, this step is performed by a subscriber accessing a web based user interface via web portal 222 on usage policy server 160.

[0109] In step 510, the user equipment 102 device registration request is sent to usage policy server 160.

[0110] In step 520, data from subscriber usage database 156 is sent from usage policy server 160 to user equipment 102 in order to synchronize. In this step, user equipment 102 is synchronized with usage policy server 160 and local store 308 is updated.

[0111] In step 530, a request to fetch values for data usage attributes is sent from user equipment 102 to usage policy server 160. Attribute/value pairs fetched in this step may include application, subscriber, and/or network-based thresholds and quotas.

[0112] In step 540, a bulk registration request is sent from usage policy server 160 to PCRF 142. In this step, a bulk registration request from usage policy server 160 comprising data usage information for a plurality of user equipment 102 that has registered with usage policy server 160 is forwarded to PCRF 142. In an embodiment, the data usage information contains threshold and stoppage policies based on criteria such as data volume and the characteristics of a home network service provider 220 or a roamed network service provider 230.

[0113] In step 545, PCRF 142 sends usage stream information comprising current data usage information for user equipment 102 to usage policy server 160.

[0114] In step 550, usage policy server 160 sends a request to PCRF 142. In this step, a request to control data usage for user equipment 102 is sent based upon a stoppage decision made by PCRF 142.

[0115] FIG. 6 depicts a flowchart 600 of an exemplary method for monitoring and controlling data usage, according to embodiments of the present invention.

[0116] FIG. 6 is described with continued reference to FIGs. 1-5. However, flowchart 600 is not limited to those embodiments.

[0117] In step 610, a user equipment 102 device registration request is sent to a usage policy server 160. In an embodiment this step is performed using interface 404 on user equipment 102. In another embodiment, this step is performed by a subscriber accessing a web based user interface via web portal 222 on usage policy server 160.

[0118] In step 620, user equipment 102 is synchronized and updated using data from subscriber usage database 156 sent from usage policy server 160. In this step, local store 308 is updated.

[0119] In step 630, values for data usage thresholds and attributes are requested from user equipment 102. In an embodiment, thresholds and attribute/value pairs are tunable or editable on user equipment using interface 404. Attribute/value pairs may include application, subscriber, and/or network-based thresholds and quotas. Thresholds may include percentage usage levels beyond which a notification is to be sent to a subscriber using user equipment 102.

[0120] In step 640, bulk registration is performed. The bulk registration includes collecting data usage information for a plurality of user equipment 102 that has registered with a usage policy server 160. The data usage information comprises threshold and stoppage policies based on criteria such as data volume and the characteristics of network service providers.

[0121] In step 650, the usage stream for a subscriber is updated. In this step, usage stream information comprising current data usage information for user equipment 102 may be sent to a usage policy server 160.

[0122] In step 660, a determination whether an attribute value obtained in step 630 has been exceeded. In this step, a determination is made whether any

attribute value has been exceeded, such as a daily MB cap, a cap by an application 306 running on user equipment 102, a cap for user equipment 102, and/or an overall data cap for a subscriber

[0123] If an attribute has not been exceeded, operation proceeds to step 665. If threshold has been exceeded, operation proceeds to step 670.

[0124] In step 665, a determination whether a threshold value obtained in step 630 has been exceeded. In this step, a determination is made whether any threshold has been exceeded, such as a percentage threshold regarding daily usage in MBs, has been reached.

[0125] If a threshold has been exceeded, operation proceeds to step 670. If threshold has not been exceeded, operation proceeds to step 680.

[0126] In step 670, a notification is sent to subscriber. In this step, a notification may comprise a prompt in interface 404, an email message, a Short Messaging Service (SMS) message, a subscriber notification posted via web portal 222, or any other notification capable of notifying a subscriber that a threshold has been exceeded.

[0127] In step 675, after the notification sent in step 670 has been received by a subscriber, a determination is made whether a service characteristic has been changed. In this step, a subscriber, in response to the notification sent in step 670, can optionally change a service tier associated with their subscription in order to alleviate either an exceeded threshold determined in step 665 or an exceeded attribute determined in step 660. In this step, an upgrade to a next service tier can be made when a subscriber is close to reaching bandwidth caps or thresholds.

[0128] If a service characteristic is modified, operation proceeds to step 680. If a service characteristics are unchanged, operation proceeds to step 685.

[0129] In step 680, current total data usage is determined for user equipment 102. In this step, data usage for applications 306 running on user equipment 102 may also be determined. After collection and calculation of data usage information is performed in this step, control is passed back to step 650.

[0130] In step 680, data usage is controlled on user equipment 102 after a subscriber opted to not modify service characteristics in step 675 and the method ends.

Example Graphical User Interfaces

[0131] FIGs. 7-11 depict a graphical user interface (GUI) for a mobile device to display data usage, edit usage limits, define tariffs, and accept special offers to change service tiers, according to embodiments of the invention.

[0132] In an embodiment of the present invention, mobile usage policy application 104 may include the exemplary interface illustrated in FIGs. 7-11. FIGs. 7-11 are described with continued reference to the embodiments illustrated in FIGs. 1-4. However, FIGs. 7-11 are not limited to those embodiments. Throughout FIGs. 7-11, displays are shown with various hyperlinks, command regions, 'turn wheels', buttons, 'slide bars', and data entry fields, which are used to initiate action, invoke routines, enter data, view data, or invoke other functionality. For brevity, only the differences occurring within the figures, as compared to previous or subsequent ones of the figures, are described below.

[0133] FIG. 7 illustrates a data usage interface 700 that allows a subscriber to view home data used 702 in home network service provider 220 as compared roamed data used 704 while roaming in roamed network service provider 230 for a given period. In the exemplary embodiment illustrated in FIG. 7, the period is 1 month (e.g., April), but as would as would be understood by those skilled in the relevant art(s) interface 700 could display other data usage periods (i.e., hourly, daily, weekly, etc). In an embodiment, interface 404 comprises interface 700.

[0134] A subscriber can set "Notify" and "Stop" limits by selecting, using input device 710, limits button 706. Similarly, a subscriber can display and set tariffs by selecting, using input device 710, tariffs button 708. Interface 700 also displays total data usage 712.

[0135] FIG. 8 illustrates a usage limits interface 800 that allows a subscriber to set data usage limits in home network service provider 220 and in roamed

network service providers 230. According to an embodiment of the invention, interface 404 comprises interface 800. A subscriber, using input device 710 or a touch screen interface within interface 800 can change usage limits 802 for one or more network service providers. In an embodiment, usage limits 802 are changeable by scrolling through different values by using 'turn wheels' within interface 800. After one or more usage limits 802 have been changed, new usage limits 802 may be saved when a subscriber, using input device 710 or a touch screen interface within interface 800 selects save button 804. Current, updated usage data is displayed when a subscriber, using input device 710 or a touch screen interface within interface 800, selects usage button 806.

[0136] FIG. 9 illustrates a tariffs interface 900 that allows a subscriber to display and define tariffs 902 for home network service provider 220 and for roamed network service providers 230. In embodiment of the invention, interface 404 comprises interface 900. In an embodiment, some pre-set tariffs 902 are provided by the network service providers and other tariffs 902 are editable by the subscriber in interface 900 in cases where the subscriber knows the tariff 902 and a network service providers cannot know the tariff.

[0137] FIG. 10 illustrates an interface 1000 for displaying data usage. Interface 1000 is an alternative embodiment of interface 700 depicted in FIG. 7. A subscriber, using slide bars 1006, can set "Notify" and "Stop" limits. According to an embodiment, a subscriber can display special offers by selecting, using input device 710, special offers button 1008. An exemplary interface for displaying and selecting special offers is described below with reference to FIG. 11.

[0138] FIG. 11 illustrates an interface 1100 for displaying special offers presented to a subscriber by a home network service provider 220 and/or roamed network service providers 230. In an embodiment, some special offers 1102 are provided by the home network service provider 220 and other special offers 1102 are offered by roamed network service providers 230. In the exemplary embodiment depicted in FIG. 11, special offers 1102 can include offers to increase the number of Short Messaging Service (SMS) text messages the

subscriber can send and receive, a 'DayPass' on a roamed network, and a 'TopUp and Go' offer to provide a certain amount of additional data usage and/or calling minutes. In an embodiment, special offers 1102 may be offered to a user for free or may be offered for sale to the subscriber. In an embodiment, a subscriber can select special offers by selecting, using input device 710, links displayed with special offers 1102. Interface 1100 also displays total data usage 712.

Example Computer System Implementation

[0139] In an embodiment of the present invention, the methods and systems of the present invention described herein are implemented using well-known computers, such as a computer 1200 shown in FIG. 12. The computer 1200 can be any commercially available and well-known computer capable of performing the functions described herein, such as computers available from International Business Machines, Apple, Sun, HP, Dell, Cray, etc.

[0140] Computer 1200 includes one or more processors (also called central processing units, or CPUs), such as processor 1210. Processor 1210 is connected to communication bus 1220. Computer 1200 also includes a main or primary memory 1230, preferably random access memory (RAM). Primary memory 1230 has stored therein control logic (computer software), and data.

[0141] Computer 1200 may also include one or more secondary storage devices 1240. Secondary storage devices 1240 include, for example, hard disk drive 1250 and/or removable storage device or drive 1260. Removable storage drive 1260 represents a floppy disk drive, a magnetic tape drive, a compact disk drive, an optical storage device, tape backup, ZIP drive, JAZZ drive, etc.

[0142] Removable storage drive 1260 interacts with removable storage unit 1270. As will be appreciated, removable storage drive 1260 includes a computer usable or readable storage medium having stored therein computer software (control logic) and/or data. Removable storage drive 1260 reads from and/or writes to the removable storage unit 1270 in a well-known manner.

IPR2025-01572
Apple EX1002 Page 957

[0143] Removable storage unit 1270, also called a program storage device or a computer program product, represents a floppy disk, magnetic tape, compact disk, optical storage disk, ZIP disk, JAZZ disk/tape, or any other computer data storage device. Program storage devices or computer program products also include any device in which computer programs can be stored, such as hard drives, ROM or memory cards, etc.

[0144] In an embodiment, the present invention is directed to computer program products or program storage devices having software that enables computer 1200, or multiple computer 1200s to perform any combination of the functions described herein

[0145] Computer programs (also called computer control logic) are stored in main memory 1230 and/or the secondary storage devices 1240. Such computer programs, when executed, direct computer 1200 to perform the functions of the present invention as discussed herein. In particular, the computer programs, when executed, enable processor 1210 to perform the functions of the present invention. Accordingly, such computer programs represent controllers of the computer 1200.

[0146] Computer 1200 also includes input/output/display devices 1280, such as monitors, keyboards, pointing devices, etc.

[0147] Computer 1200 further includes a communication or network interface 1290. Network interface 1290 enables computer 1200 to communicate with remote devices. For example, network interface 1290 allows computer 1200 to communicate over communication networks, such as LANs, WANs, the Internet, etc. Network interface 1290 may interface with remote sites or networks via wired or wireless connections. Computer 1200 receives data and/or computer programs via network interface 1290. The electrical/magnetic signals having contained therein data and/or computer programs received or transmitted by the computer 1200 via network interface 1290 also represent computer program product(s).

[0148] The invention can work with software, hardware, and operating system implementations other than those described herein. Any software, hardware, and

operating system implementations suitable for performing the functions described herein can be used.

Conclusion

[0149] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be understood by those skilled in the relevant art(s) that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined in the appended claims. It should be understood that the invention is not limited to these examples. The invention is applicable to any elements operating as described herein. Accordingly, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A method for providing data communications cost monitoring and control for a subscriber session, comprising:

receiving, at a usage policy server, a registration request associated with the subscriber session;

determining current data usage associated with the subscriber session;

receiving, at the usage policy server, one or more data usage thresholds and one or more quotas associated with the subscriber session;

collecting, at the usage policy server, data usage information associated with the subscriber session;

sending a notification to a subscriber when the subscriber exceeds a pre-determined quota during the subscriber session; and

controlling data usage for the subscriber session when the subscriber exceeds a pre-determined quota during the subscriber session

2. The method of claim 1, wherein the notification is one or more of an email message, a Short Messaging Service (SMS) message, and a prompt in a user interface.

3. The method of claim 1, wherein determining current data usage comprises:

retrieving subscriber profile data from a subscriber data repository; and

determining the whether a quota has been exceeded based on a service tier associated with the subscriber.

4. The method of claim 1, further comprising:

sending a notification to the subscriber when a pre-determined threshold is exceeded during the subscriber session.

IPR2025-01572
Apple EX1002 Page 960

5. The method of claim 4, wherein the notification is one or more of an email message, a Short Messaging Service (SMS) message, and a prompt in a user interface.

6. The method of claim 1, further comprising:

storing data usage information in a subscriber data repository.

7. The method of claim 1, further comprising:

receiving, at the usage policy server, a request to change a service tier associated with the subscriber session; and

updating a subscriber profile based upon a requested service tier change request.

8. The method of claim 1, further comprising:

receiving, at the usage policy server, a request to change a threshold associated with the subscriber session; and

updating a subscriber profile based upon a requested threshold change request.

9. The method of claim 1, further comprising:

receiving, at the usage policy server, a request to change a quota associated with the subscriber session; and

updating a subscriber profile based upon a requested quota change request.

10. The method of claim 1, wherein the one or more quotas comprise a maximum amount data usage for a period, a maximum amount of data usage for an application, a maximum amount of data usage for a group of applications, and a maximum amount of data usage for a mobile device associated with the subscriber.

11. The method of claim 1, wherein the one or more data usage thresholds comprise a percentage of data usage as compared to a quota.

12. A system for providing data communications cost monitoring and control for a subscriber session, comprising:

a usage policy server configured to receive a registration request associated with the subscriber session;

a usage policy application configured to determine current data usage associated with the subscriber session;

a receiving module configured to receive one or more data usage thresholds and one or more quotas associated with the subscriber session;

a collection module configured to collect data usage information associated with the subscriber session;

a notification module configured to notify a subscriber when the subscriber exceeds a pre-determined quota during the subscriber session; and

a control module configured to limit data usage for the subscriber session when the subscriber exceeds a pre-determined quota during the subscriber session.

13. The system of claim 12 further comprising a data usage limit module configured to receive and display modifications to data usage limits associated with the subscriber session.

14. The system of claim 13, wherein the data usage limit module is further configured receive and display modifications to data usage limits associated with one or more applications running on a mobile device.

15. The system of claim 14, wherein the data usage limit module is further configured to run on a web server.

16. The system of claim 14, wherein the data usage limit module is further configured to run on a mobile device.

17. The system of claim 12 further comprising a tariff definition module configured to receive modifications to tariffs associated with one or more network service providers.

18. The system of claim 17, wherein the tariff definition module is further configured to display modified tariffs associated with associated with one or more network service providers.

19. The system of claim 18, wherein the tariff definition module is further configured to run on a web server.

20. The system of claim 18, wherein the tariff definition module is further configured to run on a mobile device.

21. The system of claim 12 further comprising a special offer module configured to receive and display special offers to alter a service tier associated with the subscriber session.

22. The system of claim 21, wherein the special offer module is further configured receive and display special offers from a home network service provider associated with the subscriber session.

23. The system of claim 21, wherein the special offer module is further configured receive and display special offers from a roamed network service provider associated with the subscriber session.

IPR2025-01572
Apple EX1002 Page 963

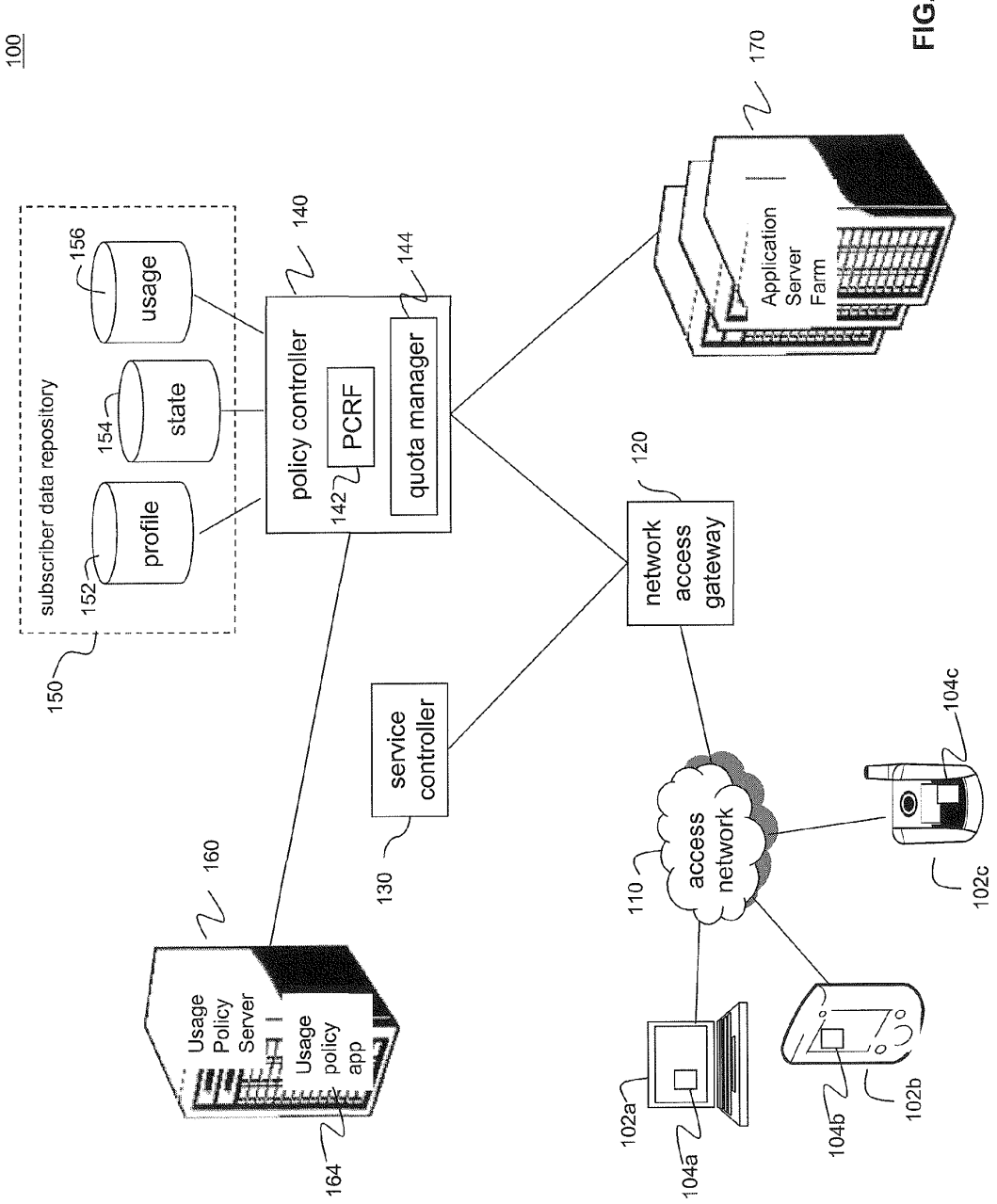

100
subscriber data repository
usage
state
profile
156
154
152
150
policy controller
PCRF
quota manager
140
142
144
Application Server Farm
170
network access gateway
120
service controller
130
Usage Policy Server
Usage policy app
160
164
access network
110
102a
104a
104b
102b
102c
104c

FIG. 1

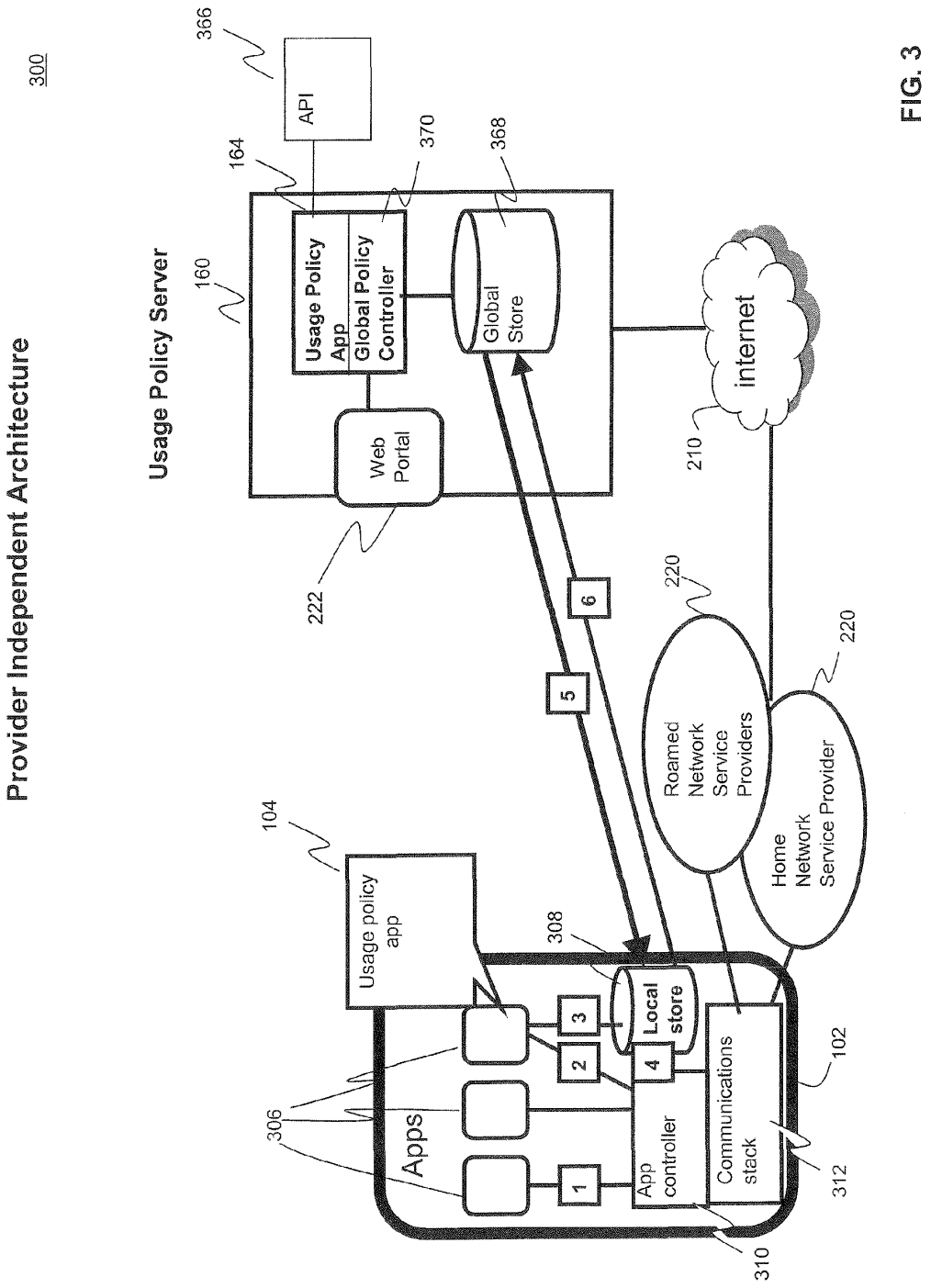

300
Provider Independent Architecture
Usage Policy Server
160
164
366
API
370
368
Usage Policy App
Global Policy Controller
Global Store
Web Portal
222
internet
210
220
Roamed Network Service Providers
220
Home Network Service Provider
104
Usage policy app
308
Local store
3
2
4
1
6
5
306
Apps
App controller
Communications stack
102
312
310

FIG. 3

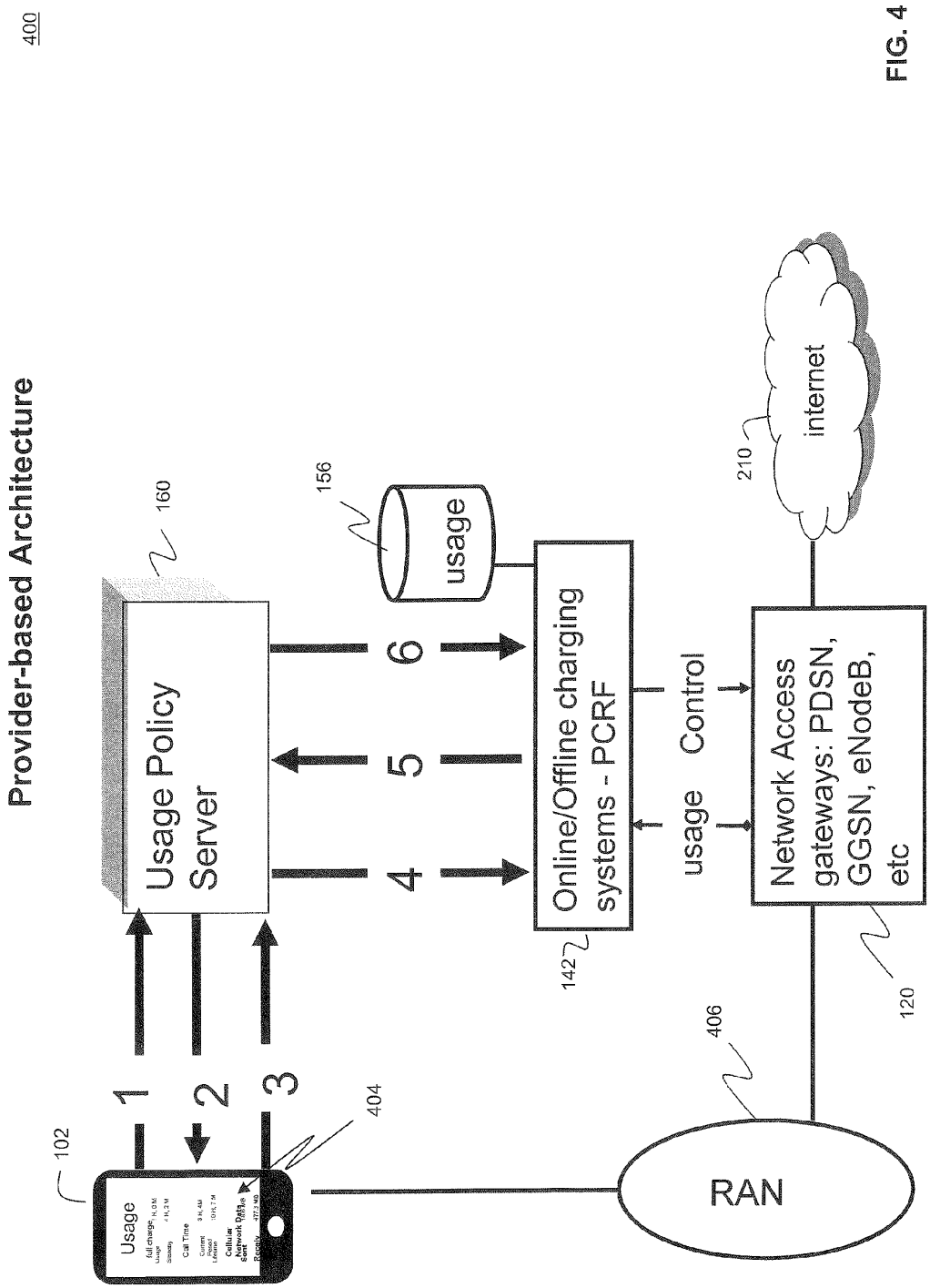


FIG. 4

IPR2025-01572
Apple EX1002 Page 967

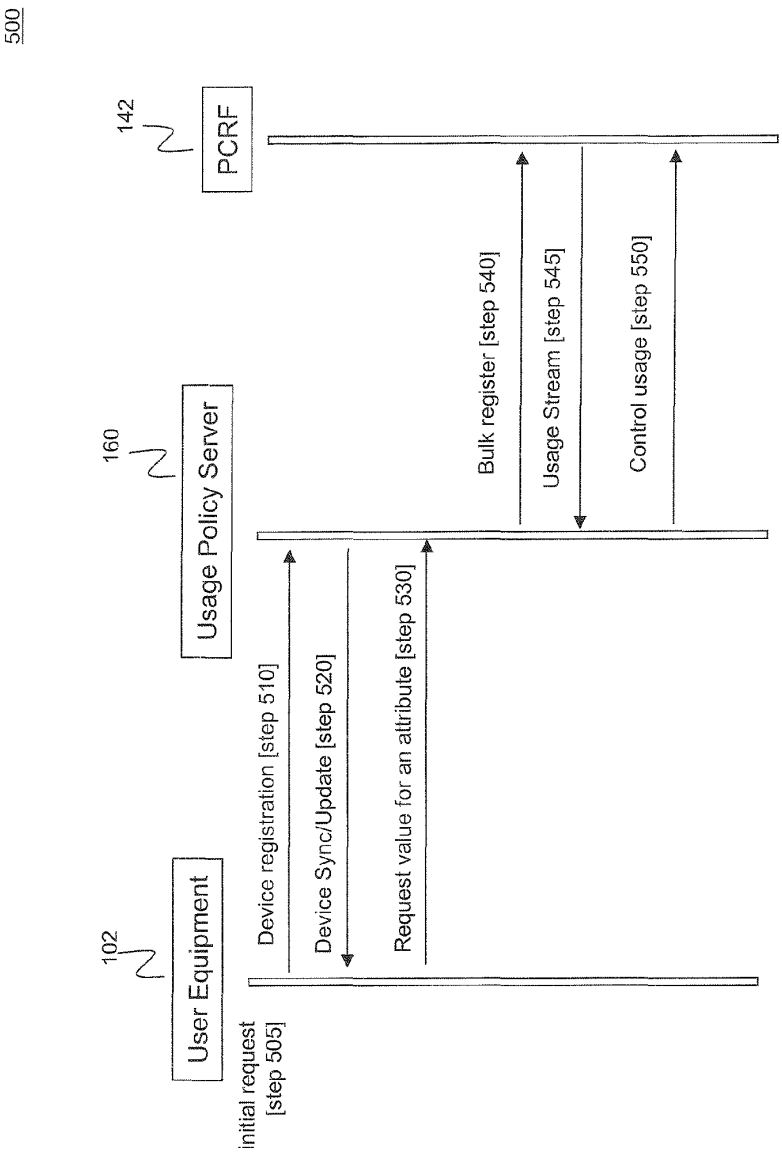

500
102
User Equipment
160
Usage Policy Server
142
PCRF
initial request [step 505]
Device registration [step 510]
Device Sync/Update [step 520]
Request value for an attribute [step 530]
Bulk register [step 540]
Usage Stream [step 545]
Control usage [step 550]

FIG. 5

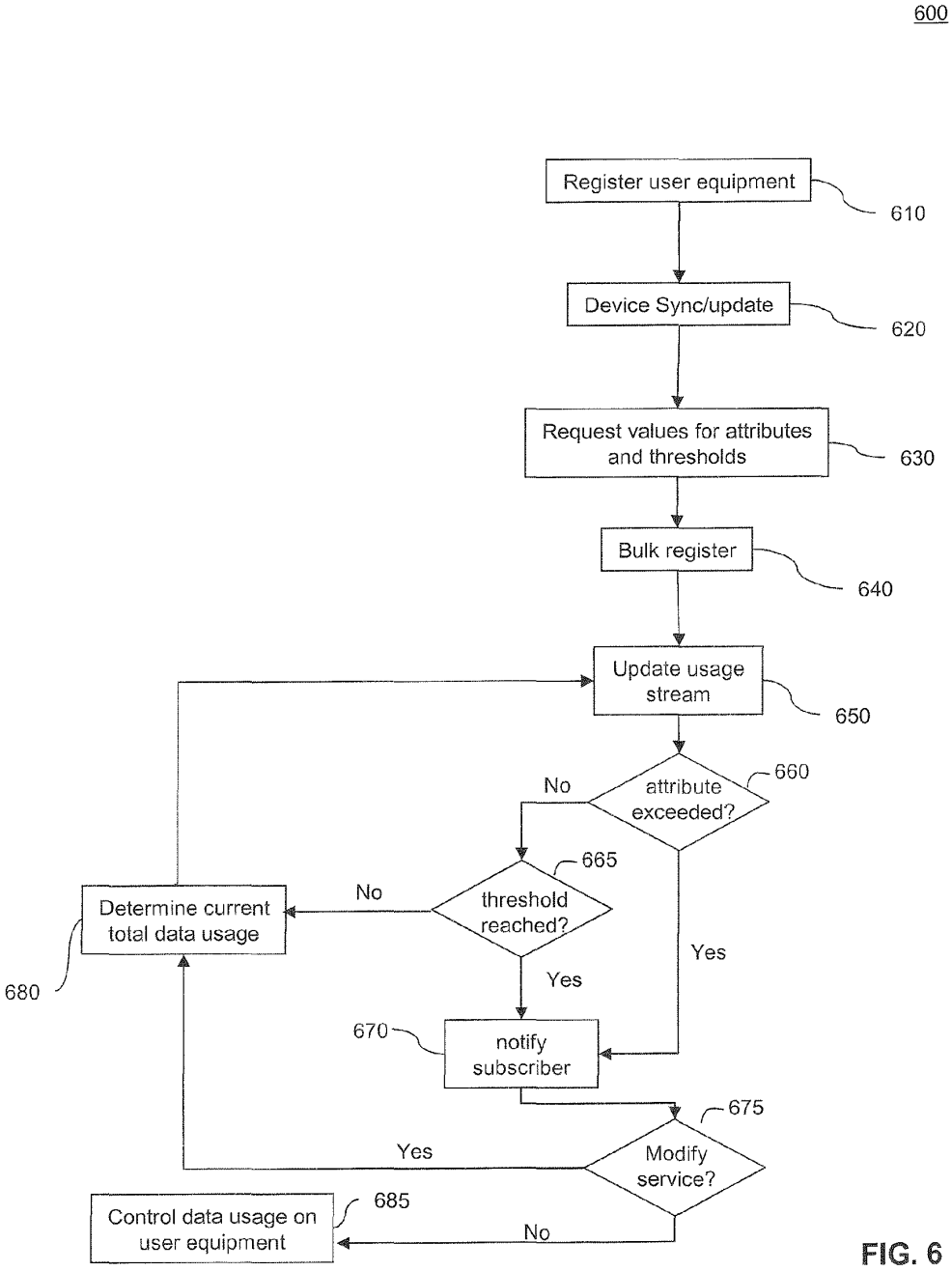

600
Register user equipment
610
Device Sync/update
620
Request values for attributes and thresholds
630
Bulk register
640
Update usage stream
650
attribute exceeded?
660
No
665
threshold reached?
No
Determine current total data usage
680
Yes
Yes
670
notify subscriber
675
Modify service?
Yes
Control data usage on user equipment
685
No

FIG. 6

Roaming Screen

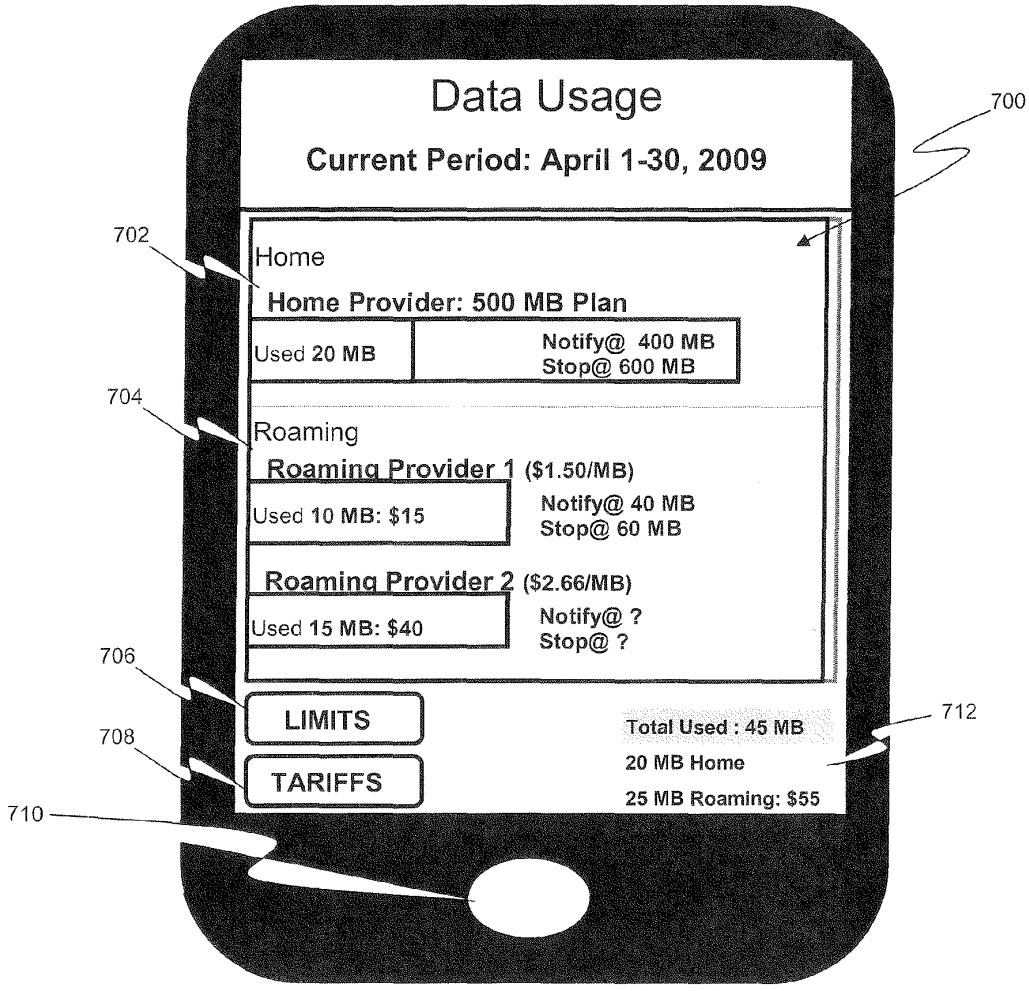


FIG. 7

Setting Usage Limits

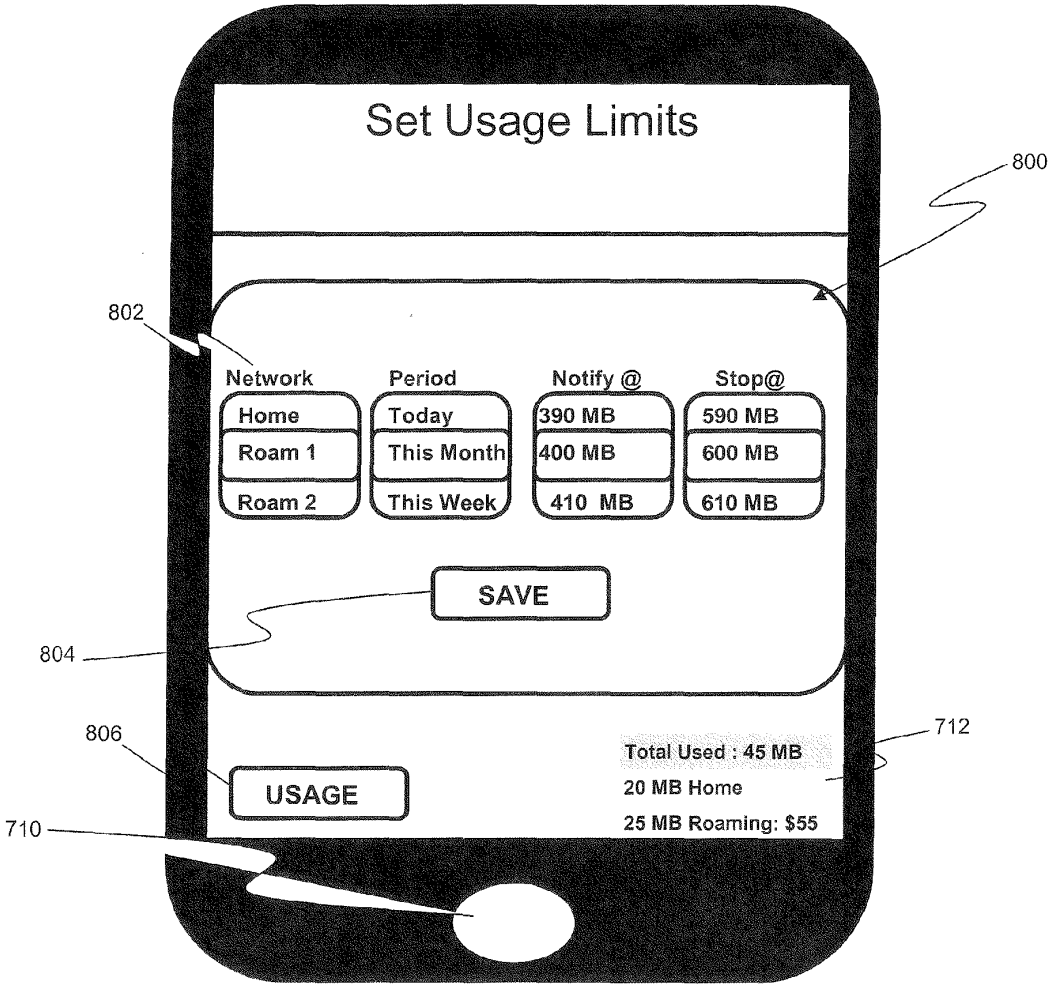


FIG. 8

Defining Tariff

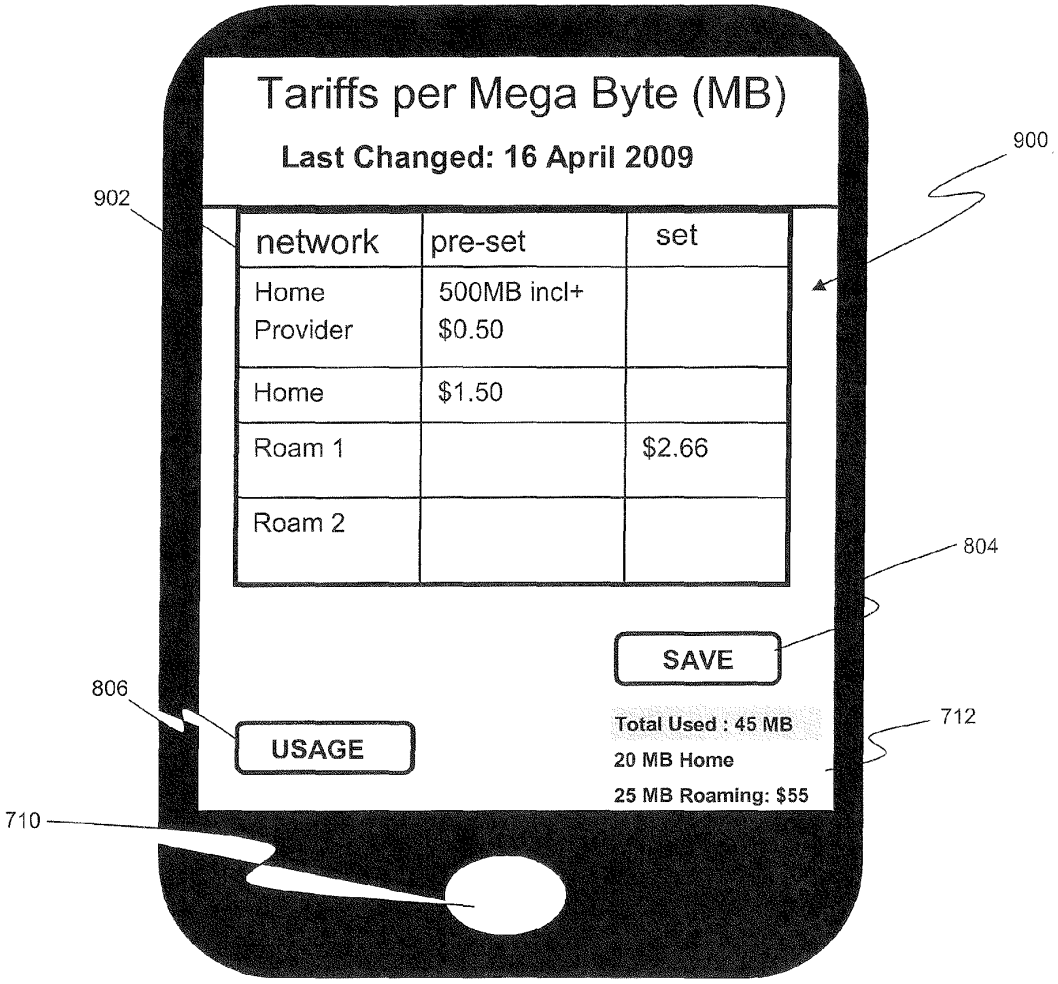


FIG. 9

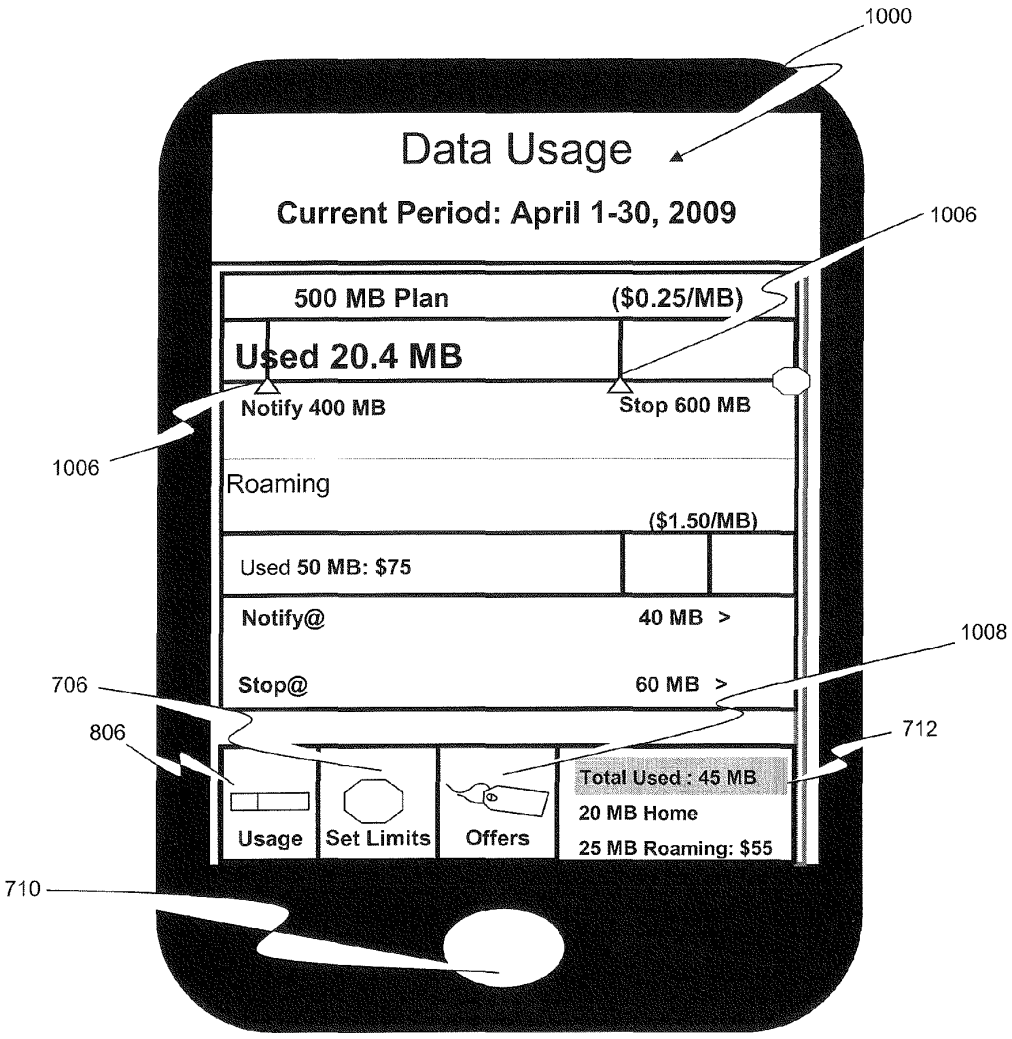

1000
Data Usage
Current Period: April 1-30, 2009
1006
500 MB Plan
($0.25/MB)
Used 20.4 MB
Notify 400 MB
Stop 600 MB
1006
Roaming
($1.50/MB)
Used 50 MB: $75
Notify@
40 MB >
1008
706
Stop@
60 MB >
806
712
Total Used : 45 MB
20 MB Home
25 MB Roaming: $55
Usage
Set Limits
Offers
710

FIG. 10

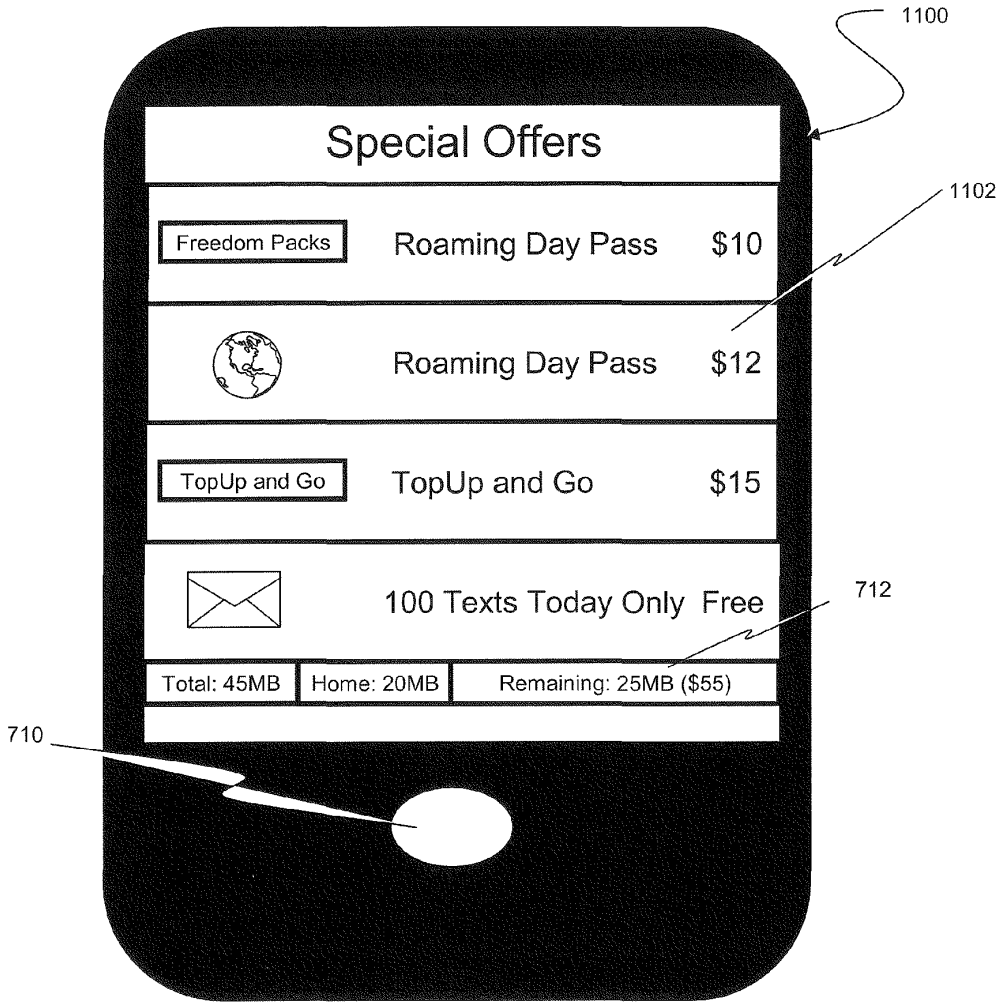

1100
Special Offers
1102
Freedom Packs
Roaming Day Pass $10
Roaming Day Pass $12
TopUp and Go
TopUp and Go $15
100 Texts Today Only Free
712
Total: 45MB
Home: 20MB
Remaining: 25MB ($55)
710

FIG. 11

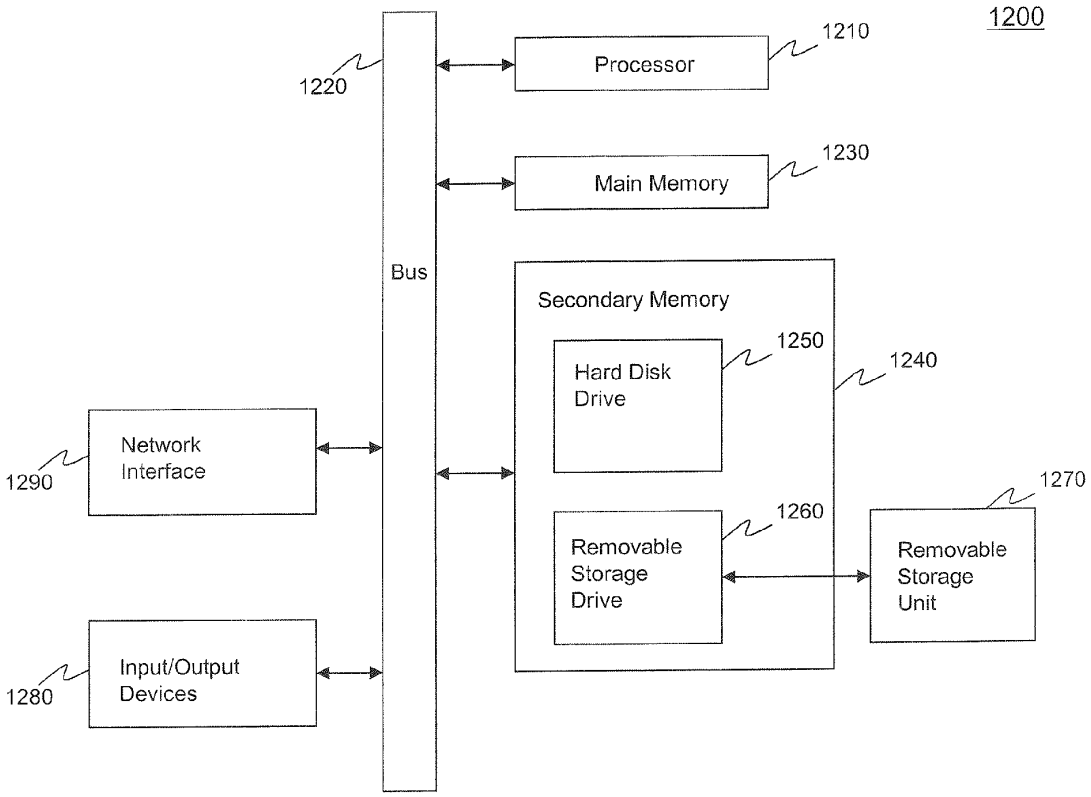

1200
1210
Processor
1220
1230
Main Memory
Bus
Secondary Memory
1250
Hard Disk Drive
1240
Network Interface
1290
1270
1260
Removable Storage Drive
Removable Storage Unit
Input/Output Devices
1280

FIG. 12

Electronic Patent Application Fee Transmittal	
Application Number:	15287597
Filing Date:	06-Oct-2016
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP041D1C1

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	120	120
		Total in USD ($)		**820**

Electronic Acknowledgement Receipt	
EFS ID:	32542188
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	06-MAY-2018
Filing Date:	06-OCT-2016
Time Stamp:	14:49:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$820
RAM confirmation Number	050718INTEFSW00018354505876
Deposit Account	505876
Authorized User	Ann Taylor
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	P041D1C1_Extension.pdf	163945 b096c983f1efaab626af876ce54520f01aa3527b	no	2
Warnings:					
Information:					
2		P041D1C1_OAR.pdf	122390 6c0bdf208318d2ed391268b21f64cbced88b6e52	yes	11
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	5	
	Applicant Arguments/Remarks Made in an Amendment		6	11	
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	P041D1C1_IDS.pdf	1055504 5c2d026d0dbe26f9c9b6ae343b91e1f908b4b536	no	11
Warnings:					
Information:					
4	Foreign Reference	2095.pdf	9614977 9f371bf4ea0c289ac564aeba3ae2f306a3292b14	no	54
Warnings:					
Information:					
5	Foreign Reference	2096.pdf	4907249 5333d14d9890f1f3087752c23cd0692d086834f1	no	30

Warnings:					
Information:					
6	Foreign Reference	2097.pdf	5055092 48ff78fc65477c69338f1ae4f44454d2354083d9	no	29
Warnings:					
Information:					
7	Foreign Reference	2098.pdf	13411096 d640be147b894d8c3f2ad40fd7969e670da1b102	no	72
Warnings:					
Information:					
8	Foreign Reference	2099.pdf	4611633 bf9b948271be5b11856ba065b36bab8ca2c283b0	no	47
Warnings:					
Information:					
9	Non Patent Literature	3070.pdf	800138 a01751f11a1220082d7b94238b19e29ecf57278e	no	37
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	32741 af7281e273f84eae414919cb68c521cde67ffad6	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	39774765	

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.

PTO/AIA/22 (03-13)
Approved for use through 7/31/2016. 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 displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): RALEP041D1C1

Application Number: 15/287,597

Filed: October 6, 2016

For: Security, Fraud Detection, and Fraud Mitigation in Device-Assisted Services Systems

Art Unit: 3687

Examiner: Rudy, Andrew J.

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.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

		Fee	Small Entity Fee	Micro Entity Fee	
☐	One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐	Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☑	Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 700
☐	Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐	Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ 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.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 505876.

☑ Payment made via EFS-Web.

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.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 40013.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/James E. Harris/ — Signature

May 6, 2018 — Date

James E. Harris — Typed or printed name

903-201-6212 — Telephone Number

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*.

☐ * Total of _____ forms are submitted.

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: Mail Stop PCT, 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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 15/287,597	Filing Date 10/06/2016	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) 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), (i), 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(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ 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

AMENDMENT **05/06/2018**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 19	Minus	** 20	= 0	X $50 =	0
Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $230 =	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

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) 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 number found in the appropriate box in column 1.

LIE
RENEE M. COLLINS

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

106963 7590 06/20/2018

Headwater Research LLC
1011 Pruitt Place
Tyler, TEXAS 75703
UNITED STATES OF AMERICA

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 06/20/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1	4727

TITLE OF INVENTION: SECURITY, FRAUD DETECTION, AND FRAUD MITIGATION IN DEVICE-ASSISTED SERVICES SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	09/20/2018

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 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity 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 and an extra copy of the form should be submitted. 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: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

IPR2025-01572
Apple EX1002 Page 985

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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 including the Patent, advance orders and notification of maintenance fees 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.

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

106963 7590 06/20/2018
Headwater Research LLC
1011 Pruitt Place
Tyler, TEXAS 75703
UNITED STATES OF AMERICA

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1	4727

TITLE OF INVENTION: SECURITY, FRAUD DETECTION, AND FRAUD MITIGATION IN DEVICE-ASSISTED SERVICES SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	09/20/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	705-300000

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/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form 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 has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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. _____

IPR2025-01572
Apple EX1002 Page 986

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.
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1	4727

106963 7590 06/20/2018

Headwater Research LLC
1011 Pruitt Place
Tyler, TEXAS 75703
UNITED STATES OF AMERICA

EXAMINER	
RUDY, ANDREW J	
ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 06/20/2018

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.

PTOL-85 (Rev. 02/11)

IPR2025-01572
Apple EX1002 Page 987

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 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, 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. 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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

Notice of Allowability	Application No. 15/287,597	Applicant(s) Raleigh et al.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA 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 the May 6, 2018 Amendment.
   ☐ 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 2-20 . 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 areply 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)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/ANDREW JOSEPH RUDY/
Primary Examiner, Art Unit 3687

IPR2025-01572
Apple EX1002 Page 989

DETAILED ACTION

Notice of Pre-AIA or AIA Status

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

Drawings

2. Applicant's Drawings submitted October 16, 2016 are acceptable.

3. Pertinent references of interest are noted on the attached PTO-892.

4. Applicant's May 6, 2018 Information Disclosure Statement (IDS) has been reviewed. Note the attached IDS.

5. Applicant cancelled claim 2.

Allowable Subject Matter

6. Claims 2-20 are allowed.

7. The following is an examiner's statement of reasons for allowance: Claims 2-20 are allowed as all the cited prior art, either alone or in combination, does not disclose Applicant's inventive claim language pursuant to Applicant's May 6, 2018 Amendment and REMARKS.

Claims 2-20 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLtweS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such.

Claims 2-20 are determined to be directed to patent-eligible subject matter and the Examiner does not consider any of the pending claims to be directed to an abstract idea. Even if the Examiner were to identify an abstract idea for any claim, then under a further analysis under Alice all claims would still be found to be patent eligible for the following reasons. The Examiner finds that when all of the elements of each claim are considered individually and as an ordered combination, each claim contains an inventive concept which is directed to an application, a particular application, or a special application, of the identified abstract idea. Further the Examiner finds that issuance of a patent for any claim would not preempt the identified abstract idea, or the field of the identified abstract idea.

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."

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Error! Unknown document property name.** whose telephone number is **Error! Unknown document property name.**. The examiner can normally be reached on **Error! Unknown document property name.**.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Fahd A. Obeid can be reached on 571-270-3324. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit 3687

Notice of References Cited	Application/Control No. 15/287,597	Applicant(s)/Patent Under Reexamination Raleigh et al.	
	Examiner ANDREW J RUDY	Art Unit 3687	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-9105031-B2	08-2015	Shen; Hui	G06Q30/02	1/1
*	B	US-8571598-B2	10-2013	Valavi; John J.	G06F1/1626	455/550.1
*	C	US-8200509-B2	06-2012	Kenedy; Andrew Alexander	G06Q50/22	705/3
*	D	US-7522549-B2	04-2009	Karaoguz; Jeyhan	H04L12/2805	370/312
*	E	US-7505756-B2	03-2009	Bahl; Pradeep	H04W12/06	370/331
*	F	US-20040019564-A1	01-2004	Goldthwaite, Scott	G06Q20/04	705/44
*	G	US-20040127256-A1	07-2004	Goldthwaite, Scott	G06K7/0004	455/558
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	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 MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/287,597	Raleigh et al.
	Examiner	Art Unit
	ANDREW J RUDY	3687

CPC - Searched*		
Symbol	Date	Examiner
H04W 12/06; H04W012/06; H04L 29/08; H04L029/08; G06F 9/445; G06F009/445; H04L 12/24; H04L012/24; H04L 29/06; H04L029/06; H04W 12/12	06/08/2018	AJR

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
370	252,351	06/08/2018	AJR
455	432.1,550.1,558	06/08/2018	AJR
705	30,300	06/08/2018	AJR
709	219-226, 238-242	06/08/2018	AJR
726	12,15	06/08/2018	AJR

* 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
Prior search updated	06/08/2018	AJR

/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	

IPR2025-01572
Apple EX1002 Page 994

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/287,597	Raleigh et al.
	Examiner	Art Unit
	ANDREW J RUDY	3687

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
H04W	12/06; 012/06; H04W 12/12	06/08/2018	AJR
H04L	H04L 29/08; H04L029/08; G06F 9/445; G06F009/445 ; H04L 12/24; H04L012/24; H04L 29/06; H04L029/06	06/08/2018	AJR
G06F	9/445; 009/445	06/08/2018	AJR

/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	

IPR2025-01572
Apple EX1002 Page 995

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/287,597	Raleigh et al.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC							
Symbol						**Type**	**Version**
H04W	/	12	/	06		F	2013-01-01
H04L	/	63	/	20		I	2013-01-01
H04L	/	63	/	0876		I	2013-01-01
H04W	/	12	/	12		I	2013-01-01
H04L	/	63	/	083		I	2013-01-01
G06F	/	8	/	65		I	2013-01-01
H04L	/	67	/	34		I	2013-01-01

CPC Combination Sets								
Symbol						**Type**	**Set**	**Ranking**	**Version**
	/		/						

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	19	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	08 June 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	35

U.S. Patent and Trademark Office — Part of Paper No.: 20180608

IPR2025-01572
Apple EX1002 Page 996

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/287,597	Raleigh et al.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

INTERNATIONAL CLASSIFICATION					
CLAIMED					
	/		/		
NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
705	300

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					
370	252					
455	432.1					
726	12					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	19	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	08 June 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	35

U.S. Patent and Trademark Office — Part of Paper No.: 20180608

IPR2025-01572
Apple EX1002 Page 997

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/287,597	Raleigh et al.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

☐ 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	2	10	10	19	20										
2	19	11	11												
3	3	12	12												
4	4	13	13												
5	5	14	14												
6	6	15	15												
7	7	16	16												
8	8	17	17												
9	9	18	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	19	
/ANDREW JOSEPH RUDY/ Primary Examiner, Art Unit 3687	08 June 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	35

U.S. Patent and Trademark Office — Part of Paper No.: 20180608

IPR2025-01572
Apple EX1002 Page 998

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. 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	15287597
Filing Date	2016-10-06
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP041D1C1

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	5915226	A	1999-06-22	Martineau	
	2	6246870	B1	2001-06-12	Dent et al.	
	3	6535949	B1	2003-03-18	Parker, Kenneth W.	
	4	6591098	B1	2003-07-08	Shieh et al.	
	5	6603975	B1	2003-08-05	Inouchi et al.	
	6	6760417	B1	2004-07-06	Wallenius, Jukka	
	7	6959202	B2	2005-10-25	Heinonen et al.	
	8	7031733	B2	2006-04-18	Alminana et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	9	7120133	B1	2006-10-10	Joo et al.	
	10	7165040	B2	2007-01-16	Ehrman et al.	
	11	7315892	B2	2008-01-01	Freimuth et al.	
	12	7548875	B2	2009-06-16	Mikkelsen et al.	
	13	7584298	B2	2009-09-01	Klinker et al.	
	14	7607041	B2	2009-10-20	Kraemer et al.	
	15	7610057	B2	2009-10-27	Bahl et al.	
	16	7620383	B2	2009-11-17	Taglienti et al.	
	17	7627600	B2	2009-12-01	Citron et al.	
	18	7656271	B2	2010-02-02	Ehrman et al.	
	19	7668966	B2	2010-02-23	Klinker et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	20	7681226	B2	2010-03-16	Kraemer et al.	
	21	7688792	B2	2010-03-30	Babbar et al.	
	22	7693107	B2	2010-04-06	De Froment, Eric	
	23	7721296	B2	2010-05-18	Ricagni, Giuseppe	
	24	7774412	B1	2010-08-10	Schnepel, Soenke	
	25	7797019	B2	2010-09-14	Friedmann	
	26	7805522	B2	2010-09-28	Schlüter et al.	
	27	7809372	B2	2010-10-05	Rajaniemi, Jaakko	
	28	7813746	B2	2010-10-12	Rajkotia, Purva R.	
	29	7835275	B1	2010-11-16	Swan et al.	
	30	7853656	B2	2010-12-14	Yach et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	31	7873346	B2	2011-01-18	Petersson et al.	
	32	7873540	B2	2011-01-18	Arumugam, Avin	
	33	7882560	B2	2011-02-01	Kraemer et al.	
	34	7930553	B2	2011-04-19	Satarasinghe et al.	
	35	7979889	B2	2011-07-12	Gladstone et al.	
	36	8024424	B2	2011-09-20	Freimuth et al.	
	37	8060017	B2	2011-11-15	Schlicht et al.	
	38	8090361	B2	2012-01-03	Hagan, Guy R.	
	39	8149748	B2	2012-04-03	Bata et al.	
	40	8234583	B2	2012-07-31	Sloo et al.	
	41	8306741	B2	2012-11-06	Tu, Ihung	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	42	8340625	B1	2012-12-25	Johnson et al.	
	43	8346923	B2	2013-01-01	Rowles et al.	
	44	8355570	B2	2013-01-15	Karsanbhai et al.	
	45	8392982	B2	2013-03-05	Harris et al.	
	46	8401968	B1	2013-03-19	Schattauer et al.	
	47	8407472	B2	2013-03-26	Hao et al.	
	48	8413245	B2	2013-04-02	Kraemer et al.	
	49	8495743	B2	2013-07-23	Kraemer et al.	
	50	8504574	B2	2013-08-06	Dvorak et al.	
	51	8531995	B2	2013-09-10	Khan et al.	
	52	8549173	B1	2013-10-01	Wu et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	53	8559369	B2	2013-10-15	Barkan	
	54	8588240	B2	2013-11-19	Ramankutty et al.	
	55	8594665	B2	2013-11-26	Anschutz, Thomas	
	56	8620257	B2	2013-12-31	Qiu et al.	
	57	8676682	B2	2014-03-18	Kalliola, Janne	
	58	8818394	B2	2014-08-26	Bienas et al.	
	59	8843849	B2	2014-09-23	Neil et al.	
	60	8849297	B2	2014-09-30	Balasubramanian	
	61	8868727	B2	2014-10-21	Yumerefendi et al.	
	62	8891483	B2	2014-11-18	Connelly et al.	
	63	8929374	B2	2015-01-06	Tönsing et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	64	9064275	B1	2015-06-23	Lu et al.	
	65	9137286	B1	2015-09-15	Yuan	
	66	9286469	B2	2016-03-15	Kraemer et al.	
	67	9286604	B2	2016-03-15	Aabye et al.	
	68	9459767	B2	2016-10-04	Cockcroft et al.	
	69	9609459	B2	2017-03-28	Raleigh, Gregory G.	

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	20020099848	A1	2002-07-25	Lee, Hoon	
	2	20040024756	A1	2004-02-05	Rickard, John Terrell	
	3	20060101507	A1	2006-05-11	Camenisch, Ja L.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

	4	20070171856	A1	2007-07-26	Bruce et al.	
	5	20100284388	A1	2010-11-11	Fantini et al.	
	6	20110004917	A1	2011-01-06	Saisa et al.	
	7	20110252430	A1	2011-10-13	Chapman et al.	

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	1098490	EP	A2	2001-05-09	Nortel Networks Ltd.		
	2	1942698	EP	A1	2008-07-09	Apple Inc.		
	3	2026514	EP	A1	2009-02-18	Nokia Siemens Networks		
	4	2007129180	WO	A2	2007-11-15	Nokia Corp.		
	5	2010128391	WO	A2	2010-11-11	Bridgewater Systems Corp.		

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

EFS Web 2.1.18

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15287597
	Filing Date	2016-10-06
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP041D1C1

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	Android Cupcake excerpts, The Android Open Source Project, Feb. 10, 2009	

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

EXAMINER SIGNATURE

Examiner Signature	/ANDREW JOSEPH RUDY/	Date Considered	06/08/2018

*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.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R./

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

BIB DATA SHEET

CONFIRMATION NO. 4727

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/287,597	10/06/2016	705	3687	RALEP041D1C1
	RULE			

APPLICANTS

Headwater Partners I LLC, Tyler, TX;

INVENTORS

Gregory G. Raleigh, Woodside, CA;
Jeffrey Green, Sunnyvale, CA;
James Lavine, Corte Madera, CA;

**** CONTINUING DATA ***************************

This application is a CON of 14/340,270 07/24/2014 PAT 9491199
which is a DIV of 13/309,463 12/01/2011 PAT 8793758
which claims benefit of 61/418,507 12/01/2010
and claims benefit of 61/418,509 12/01/2010
and claims benefit of 61/420,727 12/07/2010
and claims benefit of 61/422,565 12/13/2010
and claims benefit of 61/422,572 12/13/2010
and claims benefit of 61/422,574 12/13/2010
and claims benefit of 61/435,564 01/24/2011
and claims benefit of 61/472,606 04/06/2011
and claims benefit of 61/550,906 10/24/2011
and is a CIP of 13/237,827 09/20/2011 PAT 8832777
and is a CIP of 13/134,028 05/25/2011 PAT 8589541
and is a CIP of 13/253,013 10/04/2011 PAT 8745191
and said 13/237,827 09/20/2011
claims benefit of 61/384,456 09/20/2010
and is a CIP of 12/695,019 01/27/2010 PAT 8275830
which claims benefit of 61/270,353 07/06/2009
and claims benefit of 61/264,126 11/24/2009
and said 13/134,028 05/25/2011
claims benefit of 61/348,022 05/25/2010
and claims benefit of 61/381,159 09/09/2010
and claims benefit of 61/381,162 09/09/2010
and claims benefit of 61/385,020 09/21/2010
and claims benefit of 61/387,243 09/28/2010
and claims benefit of 61/387,247 09/28/2010
and claims benefit of 61/407,358 10/27/2010
and is a CIP of 12/694,455 01/27/2010 PAT 8402111
and is a CIP of 13/134,005 05/25/2011 PAT 8635335
and is a CIP of 12/695,021 01/27/2010 PAT 8346225
and said 12/694,455 01/27/2010
claims benefit of 61/264,120 11/24/2009
and said 12/695,021 01/27/2010
claims benefit of 61/252,153 10/15/2009
and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/134,005 05/25/2011
is a CIP of 12/380,778 03/02/2009 PAT 8321526

IPR2025-01572
Apple EX1002 Page 1008

and is a CIP of 12/380,780 03/02/2009 PAT 8839388
and said 13/253,013 10/04/2011
claims benefit of 61/389,547 10/04/2010
and is a CIP of 12/695,020 01/27/2010 PAT 8406748
and is a CIP of 12/694,445 01/27/2010 PAT 8391834
and said 12/695,020 01/27/2010
claims benefit of 61/275,208 08/25/2009
and claims benefit of 61/237,753 08/28/2009
and said 12/694,445 01/27/2010
claims benefit of 61/252,151 10/15/2009
and said 12/380,778 03/02/2009
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
and said 12/380,780 03/02/2009
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 **********************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
10/19/2016

Foreign Priority claimed ❑ Yes ☑ No 35 USC 119(a-d) conditions met ❑ Yes ☑ No Verified and Acknowledged /ANDREW JOSEPH RUDY/ Examiner's Signature	❑ Met after Allowance Initials	**STATE OR COUNTRY**	**SHEETS DRAWINGS**	**TOTAL CLAIMS**	**INDEPENDENT CLAIMS**
		CA	47	1	1

ADDRESS

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
UNITED STATES

TITLE

SECURITY, FRAUD DETECTION, AND FRAUD MITIGATION IN DEVICE-ASSISTED SERVICES SYSTEMS

FILING FEE RECEIVED 1200	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	❑ All Fees ❑ 1.16 Fees (Filing) ❑ 1.17 Fees (Processing Ext. of time) ❑ 1.18 Fees (Issue) ❑ Other _____ ❑ Credit

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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 including the Patent, advance orders and notification of maintenance fees 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.

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

106963 7590 06/20/2018
Headwater Research LLC
1011 Pruitt Place
Tyler, TEXAS 75703
UNITED STATES OF AMERICA

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Ann Taylor	(Depositor's name)
/Ann Taylor/	(Signature)
July 23, 2018	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/287,597	10/06/2016	Gregory G. Raleigh	RALEP041D1C1	4727

TITLE OF INVENTION: SECURITY, FRAUD DETECTION, AND FRAUD MITIGATION IN DEVICE-ASSISTED SERVICES SYSTEMS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	09/20/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	705-300000

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/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form 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 James. E. Harris
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 has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 505876 (enclose an extra copy of this form).

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 July 23, 2018

Typed or printed name James E. Harris Registration No. 40013

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

IPR2025-01572
Apple EX1002 Page 1010

Electronic Patent Application Fee Transmittal

Application Number:	15287597
Filing Date:	06-Oct-2016
Title of Invention:	SECURITY, FRAUD DETECTION, AND FRAUD MITIGATION IN DEVICE-ASSISTED SERVICES SYSTEMS
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Filer:	James E. Harris/Ann Taylor
Attorney Docket Number:	RALEP041D1C1

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	500	500

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**500**

Electronic Acknowledgement Receipt	
EFS ID:	33254654
Application Number:	15287597
International Application Number:	
Confirmation Number:	4727
Title of Invention:	SECURITY, FRAUD DETECTION, AND FRAUD MITIGATION IN DEVICE-ASSISTED SERVICES SYSTEMS
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP041D1C1
Receipt Date:	23-JUL-2018
Filing Date:	06-OCT-2016
Time Stamp:	15:29:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$500
RAM confirmation Number	072418INTEFSW00002106505876
Deposit Account	505876
Authorized User	Ann Taylor
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.19 (Document supply fees) 37 CFR 1.20 (Post Issuance fees)	

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P041D1C1_IssueFee.pdf	414038 c04be138b1f91c25e131ecbc0bef9f7ba2764522	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30268 d918ed1cbd4fe3e4cc32e720e9dc74824193648b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	444306		

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/287,597	08/28/2018	10064055	RALEP041D1C1	4727

106963 7590 08/08/2018

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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 0 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 Application Information Retrieval (PAIR) WEB site (http://pair.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 Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Headwater Partners I LLC, Tyler, TX;
Gregory G. Raleigh, Woodside, CA;
Jeffrey Green, Sunnyvale, CA;
James Lavine, Corte Madera, CA;

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.