



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
61/264,120	11/24/2009		220	RALEP027+		

CONFIRMATION NO. 9861

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FILING RECEIPT



OC000000039057708

Date Mailed: 12/04/2009

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. 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**

Applicant(s)

Gregory G. Raleigh, Woodside, CA;

Power of Attorney:

Michael Schallop--44319

If Required, Foreign Filing License Granted: 12/02/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/264,120**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

DEVICE ASSISTED SERVICES INSTALL

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 (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (04-07)

Approved for use through 06/30/2010 OMB 0851-0032

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

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name	Middle Name	Family Name	City	State	Country i
Gregory	G.	Raleigh	Woodside	CA	US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention	DEVICE ASSISTED SERVICES INSTALL
Attorney Docket Number (if applicable)	RALEP027+

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number ☐ Firm or Individual Name

Customer Number 21912

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

☐ Yes, applicant qualifies for small entity status under 37 CFR 1.27☒ No**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 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.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Michael J. Schallop/			Date (YYYY-MM-DD)	2009-11-24
First Name	Michael	Last Name	Schallop	Registration Number (If appropriate)	44319

This collection of information is required by 37 CFR 1.51. 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 8 hours 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. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

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 a n other 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.

DEVICE ASSISTED SERVICES INSTALL

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/206,354 (Attorney Docket No. RALEP001+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed January 28, 2009, U.S. Provisional Patent Application No. 61/206,944 (Attorney Docket No. RALEP002+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 4, 2009, U.S. Provisional Patent Application No. 61/207,393 (Attorney Docket No. RALEP003+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009, U.S. Provisional Patent Application No. 61/207,739 (Attorney Docket No. RALEP004+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on February 13, 2009, U.S. Provisional Patent Application No. 61/270,353 (Attorney Docket No. RALEP022+) entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING filed on July 6, 2009, U.S. Provisional Patent Application No. 61/275,208 (Attorney Docket No. RALEP023+) entitled ADAPTIVE AMBIENT SERVICES filed on August 25, 2009, U.S. Provisional Patent Application No. 61/237,753 (Attorney Docket No. RALEP024+) entitled ADAPTIVE AMBIENT SERVICES filed on August 28, 2009, and U.S. Provisional Patent Application No. 61/252,153 (Attorney Docket No. RALEP026+) entitled DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM filed on October 15, 2009, which are incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), DOCSIS, DSL, and Wi-Fi (Wireless Fidelity) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum and cell splitting being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0003] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0005] **Figure 1** illustrates a wireless network architecture for providing device assisted services (DAS) install techniques in accordance with some embodiments.

[0006] **Figure 2** illustrates another wireless network architecture for providing DAS install techniques in accordance with some embodiments.

[0007] **Figure 3** illustrates a flow diagram for DAS install techniques in accordance with some embodiments.

[0008] **Figure 4** illustrates another flow diagram for DAS install techniques in accordance with some embodiments.

[0009] **Figure 5** illustrates another flow diagram for DAS install techniques in accordance with some embodiments

DETAILED DESCRIPTION

[0010] 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
5 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
10 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.

[0011] A detailed description of one or more embodiments of the invention is provided
15 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
20 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.

[0012] Device assisted services (DAS) install techniques are provided in accordance with
25 some embodiments. In some embodiments, DAS install techniques for providing service processors for mobile devices are provided. In some embodiments, DAS install techniques for downloading/installing new and/or updated service processors for mobile devices are provided. In some embodiments, DAS install techniques for providing verified service processors for mobile devices are provided. In some embodiments, DAS install techniques for providing

secured service processors for mobile devices are provided. In some embodiments, DAS install techniques include a generic first version service processor used for downloading and installing a second version service processor, as described herein with respect to various embodiments.

[0013] **Figure 1** illustrates a wireless network architecture for providing device assisted services (DAS) install techniques in accordance with some embodiments. As shown, Figure 1 includes various mobile devices 100 including service processors 115. For example, mobile devices 100 can include various types of mobile phones, PDAs, computing devices, laptops, netbooks, tablets, cameras, music/media players, GPS devices, networked appliances, and any other networked device. In some embodiments, intermediate networking devices, as described herein, include a service processor or assist in the downloading of a service processor for one or more mobile devices 100 to facilitate network access as described herein with respect to various embodiments. In some embodiments, a mobile device (e.g., mobile device 100) does not initially include a service processor (as shown in Figure 1). In some embodiments, a service processor 115 is previously installed (e.g., during manufacture or distribution) or is downloaded and installed on a mobile device (as also shown in Figure 1).

[0014] In some embodiments, there are at least two versions of a service processor. For example, a first version service processor can be a generic version of a service processor version that can be pre-installed during manufacture or distribution and used for downloading a second version service processor. For example, the second version service processor can be uniquely associated with the device (e.g., mobile device 100 or an intermediate networking device) and the associated service plan and/or service provider. In some embodiments, a first version service processor is installed on a mobile device (e.g., service processor 115 installed on the mobile device 100 can be a first version service processor that was previously installed during manufacture or distribution, or downloaded and installed during initial network access, as shown in Figure 1). In some embodiments, a second version service processor is installed on a mobile device (e.g., service processor 115 can be a second version service processor that was previously installed during manufacture or distribution, or downloaded and installed during initial network access, as shown in Figure 1).

[0015] In some embodiments, a new and/or updated version service processor 115 can be downloaded from, for example, a service processor download 170, as described herein. In some embodiments, the service processor download 170 provides a function or service that is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements (e.g., the service processor download 170 can be a function/service of service control 150 and/or service policies and accounting 165). In some embodiments, the mobile devices 100 are in service control communication with service control 150 via central provider access and core networks 220. Service policies and accounting functions 165 are also provided in communication with the central provider access and core networks 220. In some embodiments, the service policies and accounting functions 165 provides a function or service that is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements (e.g., the service policies and accounting functions 165 can be a function/service of service control 150).

[0016] In some embodiments, the mobile devices 100 network access is initially restricted to service control related access (e.g., a first version service processor installed on the mobile device 100 can limit or direct network access to the service control 150, service processor download 170, and/or service policies and accounting function 165) for service processor 115 verification and/or download(s)/update(s), as described herein with respect to various embodiments. In some embodiments, after this initial restricted access period is completed and/or if the service processor 115 of the mobile device 100 is verified for the device and is current/updated, the mobile device 100 can communicate via the central provider access and core networks 220 to the Internet 120 for access to various Internet sites and/or services 240 (e.g., Google sites/services, Yahoo sites/services, Blackberry services, Apple iTunes and AppStore, Amazon.com, FaceBook, etc.) based on, for example the service plan associated with the mobile device 100. In some embodiments, service usage information (e.g., based on CDRs, micro-CDRs generated by the service processor 115, and/or other service usage measures) are used for service control and/or service plan billing and reporting, as described herein with respect to various embodiments. Those of ordinary skill in the art will appreciate that various other network architectures can be used for DAS install techniques, and Figure 1 is illustrative of just another such example network architecture for which DAS install techniques described herein can be provided.

[0017] In some embodiments, Figure 1 provides a wireless network architecture that also supports partitioned device groups, in which each device group can be provided independent and secure management. In some embodiments, partitioned device groups are provided. In some embodiments, each partitioned group of devices (e.g., mobile devices 100) can be uniquely managed with secure admin log-ins. In some embodiments, the partitioned device groups are securely managed using the service processor 115 installed on the mobile devices 100 for that device group. In some embodiments, multi-device, multi-user accounting is provided. In some embodiments, capabilities are provided to support multi-party/multi-service reconciliation records to carriers and carrier partners. In some embodiments, service usage and profitability analytics are provided. For example, a partitioned beta test group of devices can be tested and optimized for various service usage policies and/or service plans, and then the optimized service usage policies and/or service plans can be published to an entire or larger device group. In some embodiments, a carrier can be provided a carrier branded device group, and/or a MVNO can be provided a MVNO branded device group.

[0018] In some embodiments, DAS install clients (e.g., bootstrappers for mobile devices 100 and/or intermediate networking devices) are provided. In some embodiments, a first version service processor provides DAS install client function that facilitates a bootstrapping function for downloading and installing a second version service processor. In some embodiments, DAS install clients are provided for creating/downloading and installing a verifiable service processor for each device (e.g., a network capable device, such as a mobile device 100 or intermediate networking device). In some embodiments, a DAS install client downloads a uniquely secured (e.g., hashed/encrypted, such as based on device credentials to prevent, for example, mass hacking or other security vulnerabilities, and/or a signed interface between the service processor and modem) service processor for a device. In some embodiments, a non-advertised IP address allocated for each device group is rotated (e.g., to counter denial of service (DoS), distributed denial of service (DDS), and/or other types of attacks and/or vulnerabilities/exploits), and service processors are configured with multiple IP addresses for service control access (e.g., for secured network communication with service control 150 and/or service policies and accounting 165).

[0019] In some embodiments, DAS install techniques include one or more of the following operations. First, in some embodiments, whether a device is in a device group or list

that includes an installed, up to date, and/or validated service processor is determined (e.g., verify that SIM, ESN, or other unique device identifier is registered, such as in an HLR/NIR database, as associated with service settings/policies for that device for service access and send its associated charging data records (CDRs) to the service controller). Second, in some

5 embodiments, if the device does not have an installed, up to date, and/or validated service processor, then the device is directed to, for example, an activation server to, for example, authenticate the device and/or verify a service processor for the device (e.g., ensure that a current and verified service processor version is installed and/or download a current and verified service processor version for the device). For example, a DAS install client can be downloaded and

10 installed (e.g., using various bootstrapping techniques, in which, for example, during the installation of the service processor software it is sometimes necessary to update the installer or package manager itself, by using, for example, a small executable file (e.g., a bootstrapper) that updates the installer and starts the real installation after the update, and, in some cases, the bootstrapper can install other prerequisites for the service processor software during the

15 bootstrapping process as well; and using network access to a download server, and/or from a website, including, for example, service processor download function 170) that allows for secure connection from the device (e.g., mobile device 100) to a secure download server (e.g., service processor download 170). In this example, support for a configuration of the device can be determined, such as through a device query or device download of client verification software

20 can be used to verify the device hardware/software configuration). In this example, a user/device validation step can also be performed. For example, an authorization process for a user sign-up can be performed (e.g., based on a user name, MAC address, Turing machine text verification, and/or credit card verification), in which this can be performed automatically or the user/device can be required to enter certain credentials for authorization/validation. In some embodiments,

25 the authorization process also includes various security techniques for securely associating a user's identity with the device (e.g., using public key/TLS techniques, SSH techniques for TLS and/or identity management techniques). In this example, a check can also be performed to determine if the device was previously and/or is currently an activated device (e.g., the device is already associated with an active service plan). For example, whether the device belongs to a

30 registered device group can also be determined, and if not, then the default settings for that type of device can be applied. In some embodiments, the service processor is encrypted, hashed,

and/or obfuscated based on the previous determination (e.g., device group association, default device settings, and/or any other settings/criteria). In some embodiments, if the device is not associated with a service plan (e.g., based on the device look-up using device based unique identifier(s)/credential(s), as described herein), then the device can be redirected to a service portal for an activation offer for a service plan (e.g., using an activation server). In some
5 embodiments, the portal utilizes header information to indicate that the device is a managed device (e.g., for a given service provider, MVNO, or other service partner) in the portal request to proxy to an appropriate proxy server for that service provider for the activation process. Third, in some embodiments, the device is in probation mode after the new service processor
10 install (e.g., restricted a restricted IP address can be used for the service controller or other network element for service control instead of the secured service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks, such as DoS, DDS, and/or other mass attacks against publicly or other more easily accessible service controller or download servers). In some
15 embodiments, while in probation mode, the service processor executes more robust service monitoring techniques (e.g., more and/or more robust service integrity checks and/or more frequent heartbeats, for example, to monitor actual device/user behavior with the associated expected behavior, as described herein with respect to various embodiments). Fourth, in some embodiments, after a probation periods, the device is provided access based on the associated
20 service plan, which is managed, at least in part, by the service processor in communication with, for example, a service controller (e.g., service control 150 and service policies and accounting 165) or other network elements for service control.

[0020] In some embodiments, the various techniques and embodiments described herein can be readily applied to intermediate networking devices or intermediate devices (e.g., an
25 intermediate modem or networking device combination). In some embodiments, intermediate networking devices or intermediate devices include, for example, WWAN/WLAN bridges, routers and gateways, cell phones with WWAN/WLAN or WWAN/Bluetooth, WWAN/LAN or WWAN/WPAN capabilities, femto cells, back up cards for wired access routers, etc. In some embodiments, an intermediate networking device (e.g., an intermediate modem or networking
30 device combination) downloads and sends a service processor to one or more devices communicating via the intermediate device. In some embodiments, an appropriate and validated

service processor is securely downloaded to the intermediate device, and the intermediate device performs the service processor functions for the device. In some embodiments, some of the service processor functions are performed on the intermediate device (e.g., an appropriate and validated service processor is installed or securely downloaded and installed on the intermediate device), and some of the service processor functions are performed on the device itself (e.g., an appropriate and validated service processor is installed or securely downloaded and installed on the mobile device 100) (e.g., stack controls can be performed on the mobile device and various other controls can be performed on the intermediate device). In some embodiments, the mobile device cannot access the network via the intermediate device (e.g., the device is quarantined) unless the mobile device has an installed and functioning verified service processor (e.g., using CDRs from intermediate device and/or network).

[0021] In some embodiments, a USB WLAN stick or other similar networking device is provided (e.g., including a modem) with DAS install client software that loads onto the device (e.g., mobile device 100) and installs a service processor 115 on the mobile device 100. In some embodiments, software on the device instructs the user to insert a properly configured memory device (e.g., a secured USB memory stick, dongle, or other secured device that can provide a DAS install client software, a service processor image, and/or device credentials for network access). In some embodiments, the USB WLAN installed software assumes control over, for example, the network stack of the device (e.g., for managing network access) and sets various service policies based on whether the service is communicated via the USB WLAN stick or via the WiFi/other (e.g., including requiring no policies, such that access is open). In some embodiments, the DAS install client software on the USB WLAN stick provides a secure client that installs itself/certain software on the device that provides a DAS install client (e.g., bootstrapper) for the mobile device, and the DAS install client downloads an appropriate service processor onto the device and/or the USB WLAN stick (e.g., the stack can also be located and managed on the USB WLAN stick).

[0022] In some embodiments, DAS install techniques include ensuring that a device's (e.g., the device modem's) credentials for the access network match the unique credentials for the service processor and the unique credentials for the device (e.g., SIM, MZ, etc.). In some embodiments, DAS install techniques include ensuring that multiple IP addresses are not

associated with the same service processor for a particular device. In some embodiments, DAS install techniques include determining that this is the same device/modem that a service processor was previously downloaded for and whether that prior service processor is still active on the network. If so, then, in some embodiments, the user is required to type in, for example, a password to continue, for example, a reimaging of the device (or prevent the new device install or to disable the previously activated other service processor).

[0023] In some embodiments, DAS install techniques include starting with a device that does not include a service processor (e.g., a device, with, for example, a SIM or EVDO ESSN, but with no service processor, attempts to connect to the network, an appropriate service processor for the device is determined, and then a uniquely associated service processor is downloaded and installed on the device, for example, using a bootstrapper, as similarly described herein). In some embodiments, unique device credentials (e.g., MAC, SIM, etc.) are used to create a secure connection with, for example, the service controller (e.g., service control 150) or a secure download server (e.g., service processor download 170), to download a (e.g., new or replacement) service processor to be securely installed on the device. Accordingly, as described herein, DAS install techniques can be applied to at least one or more of the following situations: a new service processor install; and/or a replacement service processor install (e.g., the originally/previously installed service processor was wiped/reimaged, hardware failure, etc., and, thus, a replacement service processor is needed). In some embodiments, when a device connects to the network without, for example, a service processor, then a look up is performed (e.g., in a database) to determine whether the device is a member of a device group or a new device, and an appropriate service processor (e.g., version and settings) is provided for installation on the device. In some embodiments, when the device attempts an initial access to the network, at that time an updated version of a service processor for that device can be provided based on, for example, device type, device group, master agent, user interface (UI), settings, marketing pages, and/or other features and/or settings, which, for example, can allow for a new, changed, or evolving service plan/program by the time the device logs onto the network to provide, for example, for a dynamic and scalable solution.

[0024] In some embodiments, as similarly discussed above, two versions of the service processor are provided (e.g., a first version/image and a second version/image of the service

processor software). In some embodiments, a first version service processor is a general purpose version used, for example, primarily for connecting to the network and loading a second version service processor software that, for example, can be one or more of the following: an updated version, a version tailored to a more specific purpose (e.g., based on a device type, service type, service provider or service provider partner, or any other purpose/criteria), a version that includes additional features/functionality, an encrypted service processor version, a version that includes special service plan settings or capabilities associated with a device group, a version that includes specific branding or features/functionality for a given service provider or service provider partner associated with a device group, a version that includes special marketing materials to motivate the user to try or buy services or transactions associated with a device group, and various other versions as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein.

[0025] In some embodiments, depending on whether the user has pre-signed up for a service plan, for example, a different version of the service processor software and/or settings is/are downloaded to the device during this initial service processor download process, including, for example, one or more of the following: a different set of options for service plan choices, marketing materials, ambient service settings and service options, service plan settings, and possibly various other features and/or settings.

[0026] In some embodiments, the first version of the service processor is installed during manufacturing or in the distribution channel prior to sale of the device. In some embodiments, the first version of the service processor is installed after the time of sale of the device using various DAS install techniques as described herein with respect to various embodiments.

[0027] In some embodiments, the first version of the service processor is not uniquely encrypted so that a general purpose version of the first service processor image can be distributed to multiple devices (e.g., downloadable via the Internet, such as through a website, or a software update not installed by an operable service processor or a software image that is loaded onto the device before the device credentials or device group associations are available or known). In some embodiments, a non-encrypted generic version of the service processor is used for broad distribution to many devices in which the device credentials are not known at the time of service

processor software distribution (e.g., the generic version of the service processor can log onto the network to access a software update function in the service controller or service control 150, service processor downloader or service process download 170, and/or similar network function, then the service controller can obtain the device credentials and/or user information and provide an updated version of the service processor accordingly). In some embodiments, the second/updated version of the service processor is uniquely encrypted (e.g., based at least in part on the device credentials or device group associations). In some embodiments, a first version of the service processor need not be uninstalled and replaced by a new install of a second version of the service processor, as, in some embodiments, the second version of the service processor includes updates to the first version of the service processor, settings changes to the first version of the service processor, and/or encryption or obfuscation of the first version of the service processor to provide a second version of the service processor that is uniquely associated with the device, the device user, and/or the service plan associated with the device. In some embodiments, the second/updated version of the service processor includes one or more restricted IP addresses providing for access to the secured service control/service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks for the secured service control/service controller(s), such as DoS, DDS, and/or other mass attacks against publicly or other more easily accessible service control/service controller(s) and/or service processor download servers.

20 **[0028]** In some embodiments, the second version of the service processor is uniquely associated with some aspect(s) of the device credentials and/or user information with a temporary user account (e.g., also sometimes referred to herein as a dummy user account) or user account. In some embodiments, the second version of the service processor and/or the settings in the service processor are chosen based on a look up of some aspect of the device credentials and/or the user information to determine which device group version of the service processor and/or settings should be loaded. In some embodiments, when there is no appropriate device group association or the user preference takes priority over device group association, the first version of the service processor software is used to log onto the network (e.g., including potentially the service controller) to select a service offer, or device group association that then determines the second version and/or settings of the service processor software that will be loaded onto the device.

[0029] In some embodiments, the first version of the service processor is installed on after market devices, and after installation this more general purpose version of the service processor provides for access to the service control/service controller (or similar network function). In some embodiments, the service control/service controller determines what type of device and/or what operating system (OS) software and/or what modem and modem software is on the device, and then loads an appropriate version of the service processor for that device or facilitates an updating of the first version of the service processor to provide a second version of the service processor for that device.

[0030] In some embodiments, the service processor is distributed on a peripheral device suitable for use with more than one type of device and/or more than one type of OS. Accordingly, in some embodiments, more than one version of the service processor can be shipped with the device for installation on the device once the device type and/or OS type is/are known, with each version of the software either being a first version of the service processor software as discussed above, or a second version or final version of the service processor software as discussed above.

[0031] In some embodiments, the first version/second version service processor software techniques, for example, allow for installations of a new OS version that is not compatible in some way with the present version of the service processor. For example, the installation of such a new and incompatible OS version can render the currently installed service processor version incapable of connecting to the network and updating the service processor. In such an example, a first version service processor software image that is compatible with the new OS can be used to access the network (e.g., connect to the service control/service controller or some other network element) to download and install a new, possibly uniquely encrypted and compatible second service processor image, as similarly discussed above.

[0032] In some embodiments, the first version/second version service processor software techniques, for example, can handle situations in which a device has an inadvertently wiped or damaged service processor image such that the device is no longer capable of logging onto the network with its secure credentials and/or uniquely encrypted service processor software image.

In such an example, the first version software processor can then be used as similarly described above to download and install a new second version service processor on the device.

[0033] In some embodiments, there are multiple types of device log-in to the service control/service controller depending on whether a first or second version service processor is being used. For example, if a second version service processor is being used, which, in some embodiments, includes unique secure credentials, uniquely encrypted or secure heartbeat channel, and/or a uniquely encrypted service processor software image, then the capabilities of the device and/or service processor to access the network and/or service controller elements can be as similarly described herein with respect to various embodiments. However, if the device is using a first version service processor, which, for example, does not have unique secure credentials, a uniquely encrypted heartbeat control channel, and/or a uniquely encrypted software image, then the heartbeat control channel traffic can be handled in a differential manner as compared to the traffic handling implemented for a second version service processor image. For example, the service controller heartbeat processing elements can detect that the service processor is a first version service processor and can then route the heartbeat traffic through a different set of security processes that do not rely on all the security aspects present in a second version service processor. As another example, the first version service processor can be a widely distributed software image that does not have unique encryption on the heartbeat channel and can be handled differentially, such as handled with a different server designed to handle insecure traffic and designed to not be disposed or easily exposed to mass attacks (e.g., DoS, DDS attacks, and other types of security related and/or mass/large scale attacks against a network element, such as a download server or web/application server).

[0034] In some embodiments, a device supports two or more operating systems (e.g., different versions of operating systems and/or different operating systems) and for each operating system includes a compatible service processor. For example, when a dual boot configured device boots in a first operating system version, then a first service processor that is compatible with that first operating system version is selected for network access, and when the dual boot configured device boots in a second operating system version, then the second service processor that is compatible with that second operating system version is selected for network access.

[0035] In some embodiments, initial network access for a device is directed to a service controller (e.g., service control 150), service processor downloader (e.g., service processor download 170), and/or similar network element for managing service control. In some embodiments, initial network access is restricted to this initial network access to the service controller, service processor downloader, and/or similar network element for managing service control. In some embodiments, such initial network access is restricted until the device has been verified for network access, as similarly discussed herein with respect to various embodiments. In some embodiments, such initial network access is restricted until the device has been verified for network access and an appropriate service processor has been verified on the device and/or downloaded and installed on the device, as similarly discussed herein with respect to various embodiments. In some embodiments, such initial network access is restricted using various techniques, such as using a first version of a service processor on the device that restricts such initial network access. In some embodiments, such initial network access is restricted to and maintained in probation mode, as similarly described herein (e.g., a restricted IP address can be used for the service controller or other network element for service control instead of the secured service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks, such as DoS, DDS, and/or other mass attacks against publicly or other more easily accessible service controller or download servers). For example, such initial network access can include access to a common activation server, which the device can access for determination of a supported configuration for a new or second service processor image download. As another example, such initial network access can direct the device to an initial web page including access to a service plan offer and purchase options (e.g., providing for a device credential look up for device group, provide choices of programs to user, etc.). As another example, the initial web page can include access to a service plan offer and purchase options and a service processor verification and download/update function.

[0036] In some embodiments, a network based charging data records (CDR) feed, as described with respect to various embodiments, is provided for monitoring service usage by managed devices. In some embodiments, the CDR feed includes micro-CDRs generated by the service processor (e.g., service processor 115) on the device (e.g., mobile device 100 or an intermediate networking device for that mobile device). In some embodiments, the CDR feed is

a real-time (e.g., near real-time) network based CDR feed is provided for determining whether any devices have been compromised (e.g., a hack of a first version or second version service processor providing for unrestricted service usage for such devices, and/or any other mass or security attack or vulnerability or exploit). For example, such a CDR feed can be used to
5 determine abnormal or unusual traffic patterns and/or service level usage activities, which, for example, can be used to identify and/or protect against a DoS/DDS attack or other types of security attacks.

[0037] In some embodiments, based on various device and/or network based monitoring techniques, as described herein with respect to various embodiments, a determination is made
10 that the service processor (e.g., service processor 115) is not functioning properly (e.g., may have been damaged and/or compromised/tampered with and, for example, allowing network access beyond the device's associated service plan and/or not properly monitoring/billing for such service usage) and that a new/replacement service processor should be downloaded. In some embodiments, a new/replacement service processor can be downloaded and installed in such
15 situations, using the various techniques described herein with respect to various embodiments. In some embodiments, based on various criteria (e.g., service usage monitoring, billing, and/or any other criteria) or based on proactive and/or periodic administrative/security measures, a new/replacement service processor can be downloaded and installed, using the various techniques described herein with respect to various embodiments.

[0038] In some embodiments, based on, for example, service plan changes (e.g., user changes to their service plan), service provider changes (e.g., service provider changes to their services/service policies or the associated service plan), device changes (e.g., operating system version or other software platform changes or various hardware changes), a new service processor can be downloaded and installed or the installed service processor can be updated,
25 using the various techniques described herein with respect to various embodiments.

[0039] **Figure 2** illustrates another wireless network architecture for providing DAS install techniques in accordance with some embodiments. As shown, Figure 2 includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless mobile devices 100 are in communication with base stations 125 for wireless network

communication with the wireless network, and other devices 100 are in communication with Wi-Fi Access Points (APs) or Mesh 702 for wireless communication to Wi-Fi Access CPE 704 in communication with central provider access network 109. In some embodiments, each of the mobile devices 100 includes a service processor 115 (as shown), which, for example, can be initially installed, downloaded, and/or updated service processors (e.g., first/second version service processor images) using service processor download function 170 as described herein, and each service processor 115 connects through a secure control plane link to a service controller 122. In some embodiments, the service processor download function 170 is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements as will be apparent to one of ordinary skill in the art in view of the various embodiments disclosed herein.

[0040] In some embodiments, service usage information includes network based service usage information (e.g., charging data records (CDRs)), which is obtained from one or more network elements. In some embodiments, service usage information includes micro-CDRs provided by the service processor (e.g., service processor 115) installed on the device (e.g., mobile device 100). In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired, as described herein with respect to various embodiments. In some embodiments, each device activity that is desired to be associated with a billing event is assigned a micro-CDR transaction code, and the service processor 115 is programmed to account for that activity associated with that transaction code. In some embodiments, the service processor 115 periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, the service controller 122 or some other network element. In some embodiments, the service controller 122 reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN) and then transmits it to CDR mediation. In some embodiments, CDR mediation is used to account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions for CDR mediation and billing. For example, the billing system processes the mediated CDR feed from CDR mediation, applies the appropriate

account billing codes to the aggregated micro-CDR information that was generated by the device, and then generates billing events in a manner that does not require changes to billing systems (e.g., using new transaction codes to label the new device assisted billing capabilities).

[0041] As shown in Figure 2, a CDR storage, aggregation, mediation, feed 118 is provided (and other network elements as shown in Figure 2). In some embodiments, the CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100. In some embodiments, the CDR storage, aggregation, mediation, feed 118 also provides a settlement platform using the mediated micro-CDRs, as described herein with respect to various embodiments. In some embodiments, another network element provides the settlement platform using aggregated and/or mediated micro-CDRs (e.g., central billing interface 127 and/or another network element). In some embodiments, various techniques for partitioning of device groups are used for partitioning the mobile devices 100 (e.g., allocating a subset of mobile devices 100 for a distributor, an OEM, a MVNO, and/or another partner). As also shown, a MVNO core network 210 also includes a MVNO CDR storage, aggregation, mediation, feed 118, a MVNO billing interface 122, and a MVNO billing system 123 (and other network elements as shown in Figure 2). In some embodiments, the MVNO CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100 (e.g., MVNO group partitioned devices). Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing DAS install techniques, and Figure 2 is illustrative of just one such example network architecture for which DAS install techniques described herein can be provided.

[0042] In some embodiments, CDR storage, aggregation, mediation, feed 118 (e.g., service usage 118, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment boxes attached to one or more of the sub-networks shown in Figure 2 (e.g., central provider access network 109 and/or central provider core network 110), which is in communication with the service controller 122, and a central billing interface 127. As shown, service usage 118 provides a function in communication with the central provider core network 110. In some embodiments, the CDR storage, aggregation, mediation, feed 118 function is

located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in the AAA server 121 and/or the mobile wireless center/Home Location Register (HLR) 132 (as shown, in communication with a DNS/DHCP server 126). In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base station aggregator, collectively referred to as base station 125 in Figure 2. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in a networking component in the central provider access network 109, a networking component in the core network 110, the central billing system 123, the central billing interface 127, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed 118) can be easily generalized as described herein and as shown in the other figures described herein by one of ordinary skill in the art. Also as shown in Figure 2, the service controller 122 is in communication with the central billing interface 123 (also sometimes referred to as the external billing management interface or billing communication interface) 127, which is in communication with the central billing system 123. As shown, an order management 180 and subscriber management 182 are also in communication with the central provider core network 110 for facilitating order and subscriber management of services for the devices 100 in accordance with some embodiments.

[0043] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) collects device generated usage information for one or more devices on the wireless network (e.g., devices 100); and provides the device generated usage information in a syntax and a communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, as described herein, the CDR

storage, aggregation, mediation, feed 118 collects/receives micro-CDRs for one or more devices on the wireless network (e.g., devices 100). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated usage information. In some embodiments, the network device is a CDR feed aggregator, and the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) also aggregates CDRs and/or micro-CDRs for the one or more devices on the wireless network; applies a set of rules to the aggregated CDRs and/or micro-CDRs using a rules engine (e.g., bill by account, transactional billing, revenue sharing model, and/or any other billing or other rules for service usage information collection, aggregation, mediation, and reporting), and communicates a new set of CDRs for the one or more devices on the wireless network to a billing interface or a billing system (e.g., providing a CDR with a billing offset by account/service).

[0044] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates a new set of CDRs (e.g., aggregated and mediated CDRs and/or micro-CDRs that are then translated into standard CDRs) for the one or more devices on the wireless network to a billing interface (e.g., central billing interface 127) or a billing system (e.g., central billing system 123). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller (e.g., service controller 122) to collect the device generated usage information (e.g., micro-CDRs) for the one or more devices on the wireless network. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller, in which the service controller is in communication with a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates the device generated usage information to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated usage information for the one or more devices on the wireless network. In some

embodiments, the service controller 122 communicates the device generated service usage information (e.g., micro-CDRs) to the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements).

5 [0045] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs rules for performing a service billing function, as described herein, and/or for performing a service/transactional revenue sharing function, as described herein. In some
10 embodiments, the service controller 122 in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device generated usage information (e.g., micro-CDRs). In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations
15 of network elements) performs a rules engine for aggregating and mediating the device generated usage information.

[0046] In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed 118. In some embodiments, the rules engine and associated functions, as discussed herein, is a separate function/device. In some
20 embodiments, the service controller 122 performs some or all of these rules engine based functions, as discussed herein, and communicates with the central billing interface 127. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as discussed herein, and communicates with the central billing system 123.

[0047] In some embodiments, duplicate CDRs are sent from the network equipment to
25 the billing system 123 that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., the managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system 123.

[0048] In some embodiments, the service controller 122 sends the device generated CDRs to the rules engine (e.g., service usage 118), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller 122 generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface 127. For example, for the service controller 122 to generate CDRs similar to other network elements, in some embodiments, the service controller 122 is provisioned on the wireless network and behaves substantially similar to other CDR generators on the network) as would be apparent to one of ordinary skill in the art.

[0049] In some embodiments, the service controller 122 is provisioned as a new type of networking function that is recognized as a valid and secure source for CDRs by the other necessary elements in the network (e.g., CDR storage, aggregation, mediation, feed 118). In some embodiments, where the network necessary apparatus will only recognize CDRs from certain types of networking equipment (e.g. RAN Gateway 410 or Transport Gateway 420), then the Service Controller 122 can provide authentication credentials to the other networking equipment that indicate it is one of the approved types of equipment. In some embodiments, the link between the Service Controller 122 and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted and/or signed.

[0050] In some embodiments, the CDR storage, aggregation, mediation, feed 118 discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller 122 can provide the device based service usage information (e.g., device based CDRs or micro-CDRs) to the CDR storage, aggregation, mediation, feed 118 (e.g., the CDR storage, aggregation, mediation, feed 118 can just provide a store, aggregate, and communication function(s)), and the device based service usage information is provided to the central billing interface 127 or the central billing system 123.

[0051] In some embodiments, the device based CDRs (e.g., micro-CDRs) and/or new CDRs generated based on execution of a rules engine as described herein are provided only for devices that are managed and/or based on device group, service plan, or any other criteria,

categorization, and/or grouping, such as based on ambient service or ambient service provider or transactional service or transactional service provider.

[0052] In some embodiments, based on, for example, service plan changes (e.g., user changes to their service plan), service provider changes (e.g., service provider changes to their services/service policies or the associated service plan), micro-CDR transaction code changes, and/or any other related changes, a new service processor can be downloaded and installed or the installed service processor can be updated to allow, for example, the tracking of one or more service usage activities by the device using micro-CDRs (e.g., for new or previously unmonitored/untracked service usage activities, using, for example, new or updated micro-CDR transaction codes (uniquely) associated with such service usage activities), using the various techniques described herein with respect to various embodiments.

[0053] **Figure 3** illustrates a flow diagram for DAS install techniques in accordance with some embodiments. At 302, the process begins. At 304, whether a device (e.g., mobile device 100) is in a device group is determined (e.g., or other list that indicates that this device includes an installed, up to date, and/or validated service processor, and, for example, to also verify that the SIM, ESN, or other unique device identifier is registered, such as in an HLR/NIR database, as associated with service settings/policies for that device for service access and send its associated charging data records (CDRs) to the service control/service controller). At 306, whether the device includes a service processor is determined. If so, at 308, then the installed service processor is verified (e.g., up to date and/or validated for that device, device group, and/or associated service plan) and network access is allowed (e.g., managed/monitored by the installed service processor according to the associated service plan for the device). Otherwise (e.g., the device does not have an installed service processor), at 310, then an appropriate service processor for the device is determined (e.g., based on the device type, device group, and/or version, such as hardware/software platform of the device, an associated service plan, service provider, and/or any other criteria or settings). At 312, the service processor is downloaded and installed (e.g., using a bootstrap process, as described herein with respect to various embodiments) and network access is allowed (e.g., managed/monitored by the installed service processor according to the associated service plan for the device). In some embodiments, the device is also directed to, for example, an activation server to, for example, authenticate the

device and/or verify a service processor for the device (e.g., ensure that a current and verified service processor version is installed and/or download a current and verified service processor version for the device) prior to allowing such network access. For example, a DAS install client can be downloaded (e.g., using bootstrapping techniques, from a download server and/or from a website) that allows for secure connection from the device (e.g., mobile device 100) to a secure download server (e.g., service processor download 170) (e.g., support for a configuration of the device is determined, such as through a device query or device download of client verification software can be used to verify the device hardware/software configuration). In this example, a user/device validation step can also be performed. For example, an authorization process for a user sign-up can be performed (e.g., based on a user name, MAC address, Turing machine text verification, credit card verification, and/or other techniques), in which this can be performed automatically or the user/device can be required to enter certain credentials for authorization/validation. In some embodiments, the authorization process also includes various techniques for associating a user's identity with the device (e.g., using public key/TLS techniques, SSH techniques for TLS and/or identity management techniques). In this example, a check can also be performed to determine if the device was previously and/or is currently an activated device (e.g., the device is already associated with a service plan). For example, whether the device belongs to a registered device group can be determined, and if not, then the default settings for that type of device can be applied. In some embodiments, the service processor is encrypted, hashed, and/or obfuscated based on the previous determination (e.g., device group association and/or default device settings). In some embodiments, if the device is not associated with a service plan (e.g., based on the device look-up using device based unique identifier(s)/credential(s), as described herein), then the device can be redirected to a service portal for an activation offer for a service plan (e.g., using an activation server). In some embodiments, the portal utilizes header information to indicate that the device is a managed device (e.g., for a given service provider, MVNO, or other service partner) in the portal request to proxy to an appropriate proxy server for that service provider for the activation process. At 314, the process is completed.

[0054] **Figure 4** illustrates another flow diagram for DAS install techniques in accordance with some embodiments. At 402, the process begins. At 404, whether a device (e.g., mobile device 100) is in a device group is determined (e.g., or other list that indicates that this

device includes an installed, up to date, and/or validated service processor, and, for example, to also verify that the SIM, ESN, or other unique device identifier is registered, such as in an HLR/NIR database, as associated with service settings/policies for that device for service access and send its associated charging data records (CDRs) to the service controller). At 406, whether
5 the device includes a first version service processor is determined. If not (e.g., the device does not have an installed first version service processor), at 408, then a new service processor is downloaded (e.g., as similarly discussed above with respect to Figure 3) and network access is allowed (e.g., managed/monitored by the installed new service processor according to the associated service plan for the device). Otherwise (e.g., the device includes an installed first
10 version service processor), then at 410, an appropriate second version service processor for the device is determined (e.g., based on the device type and version, such as hardware/software platform, device group, an associated service plan, service provider, and/or any other criteria or settings). At 412, the second version service processor (e.g., secured for the device, using various techniques, as described herein) is downloaded and installed (e.g., using bootstrapping
15 techniques, as described herein), or in some embodiments, the first version of the service processor is updated to provide a second version service processor uniquely associated with the device, and network access is allowed (e.g., managed/monitored by the installed second version service processor according to the associated service plan for the device). At 414, the process is completed.

20 **[0055]** **Figure 5** illustrates another flow diagram for DAS install techniques in accordance with some embodiments. At 502, the process begins. At 504, whether a device (e.g., mobile device 100) is in a device group is determined (e.g., or other list that indicates that this device includes an installed, up to date, and/or validated service processor, and, for example, to also verify that the SIM, ESN, or other unique device identifier is registered, such as in an
25 HLR/NIR database, as associated with service settings/policies for that device for service access and send its associated charging data records (CDRs) to the service controller). At 506, whether the device includes a first version service processor is determined. If not (e.g., the device does not have an installed first version service processor), at 508, then a new service processor is downloaded (e.g., as similarly discussed above with respect to Figure 3) and network access is
30 allowed (e.g., managed/monitored by the installed new service processor according to the associated service plan for the device). Otherwise (e.g., the device includes an installed first

version service processor), at 410, then an appropriate second version service processor for the device is determined (e.g., based on the device type and version, such as hardware/software platform, device group, an associated service plan, service provider, and/or any other criteria or settings). At 512, the second version service processor (e.g., secured using various techniques, as described herein) is downloaded and installed (e.g., using a bootstrap process, as described herein). At 514, network access is allowed in probation mode, as described herein with respect to various embodiments. For example, the device can be managed in probation mode after the new/second version service processor install (e.g., service control communication can be limited to a particular set of probation mode IP addresses that can be used for the service controller or other network element for service control instead of the secured service controller IP addresses reserved for validated and non-probation mode service processors, which, for example, can reduce the risks of various security risks, such as DoS, DDS, or other mass attacks against publicly or other more easily accessible service controller or download servers). In some embodiments, while in probation mode, the service processor executes more robust service monitoring techniques (e.g., more and/or more robust service integrity checks and/or more frequent heartbeats, for example, to monitor actual device/user behavior with the associated expected behavior). At 516, after the probation period is completed (e.g., based on time, monitored activities, and/or any other criteria), network access is allowed in normal mode (e.g., the device is no longer operating in the probation mode, as described herein). For example, after a probation period is completed (e.g., based on time, monitored activities, and/or any other criteria), the device is provided access based on the associated service plan, which is managed, at least in part, by the service processor in communication with, for example, a service controller or other network element for service control. At 518, the process is completed.

[0056] Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

DEVICE ASSISTED SERVICES INSTALL

ABSTRACT OF THE DISCLOSURE

[0057] Device assisted services (DAS) install techniques are provided in accordance with some embodiments. In some embodiments, DAS install techniques for providing service processors for mobile devices are provided. In some embodiments, DAS install techniques for downloading/installing new and/or updated service processors for mobile devices are provided. In some embodiments, DAS install techniques for providing verified service processors for mobile devices are provided. In some embodiments, DAS install techniques for providing secured service processors for mobile devices are provided. In some embodiments, DAS install techniques include a generic first version service processor used for downloading and installing a second version service processor, as described herein with respect to various embodiments.

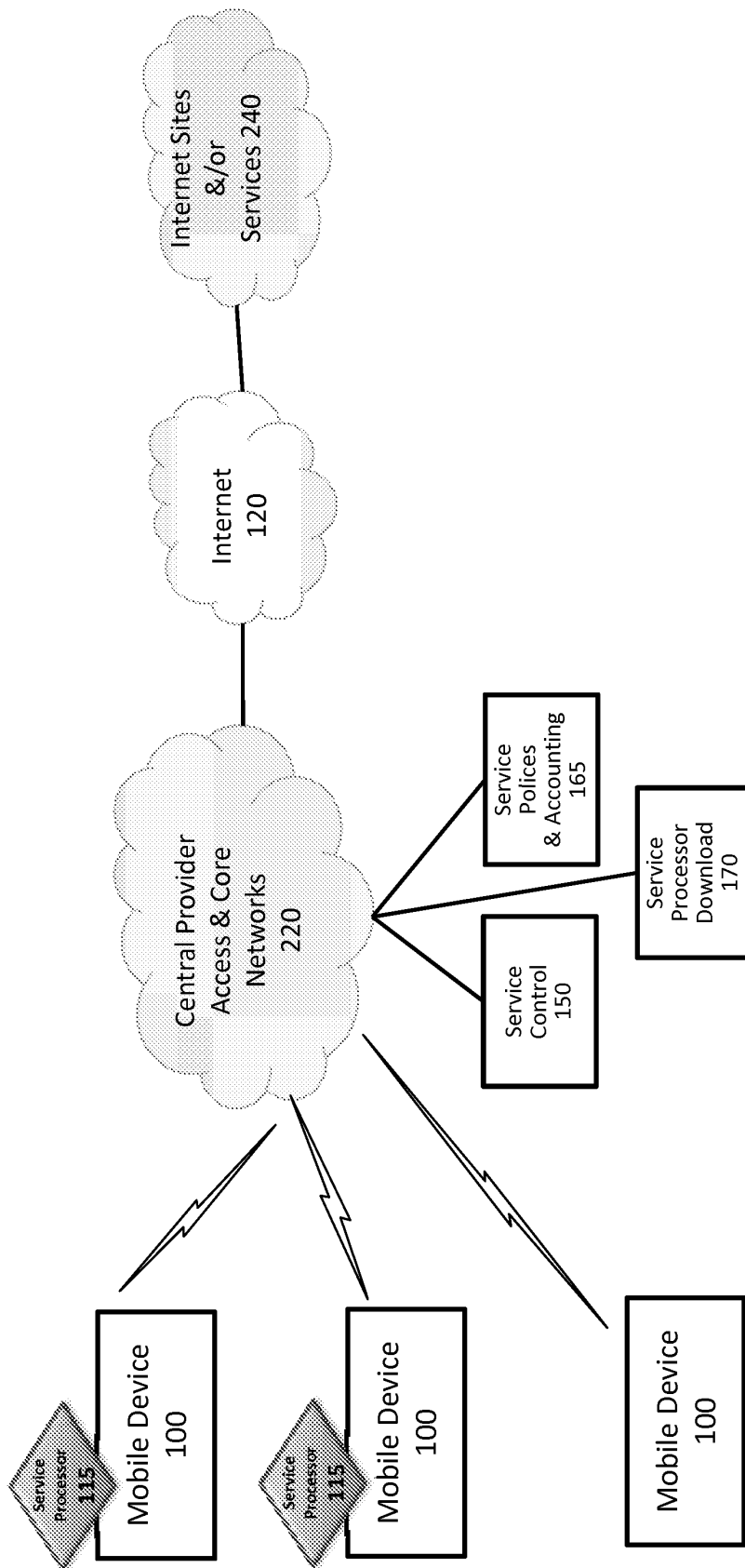


Figure 1

Figure 2

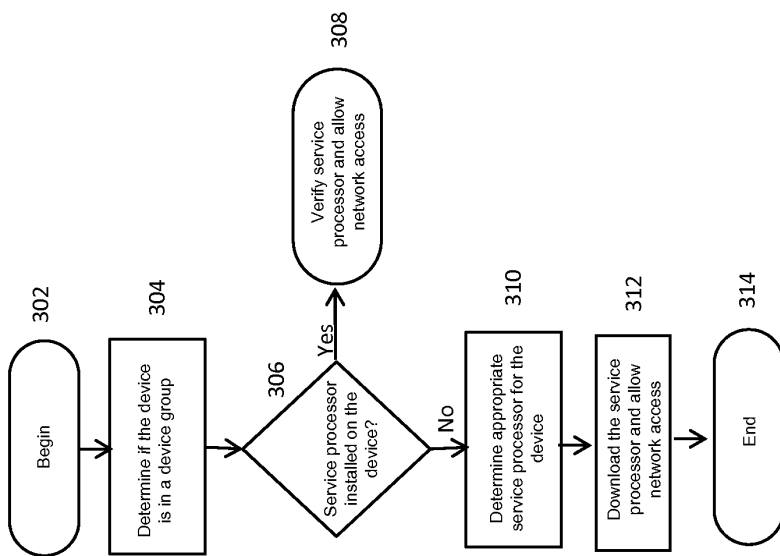


Figure 3

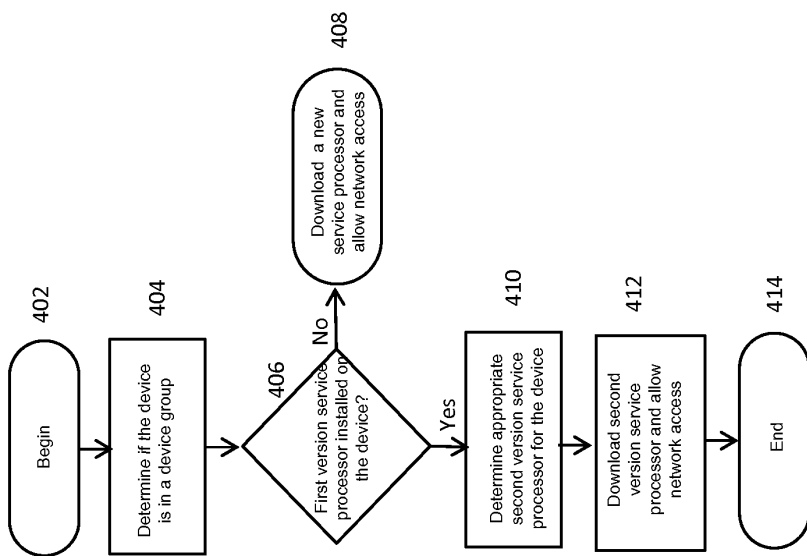


Figure 4

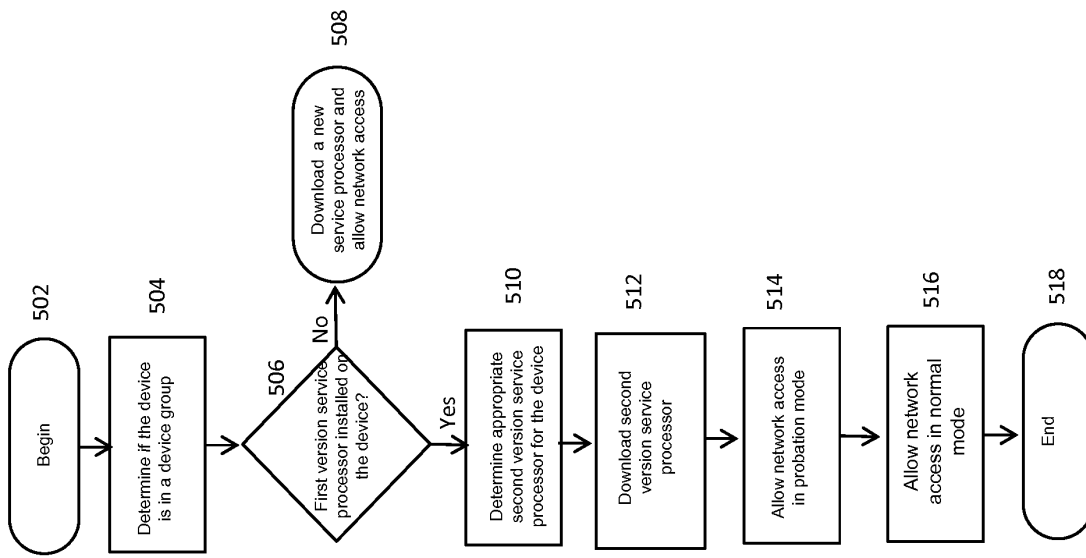


Figure 5

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		DEVICE ASSISTED SERVICES INSTALL		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		Michael J. Schallop/Veronica Pula		
Attorney Docket Number:		RALEP027+		
Filed as Large Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional application filing	1005	1	220	220
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(\$)
Miscellaneous:				
Total in USD (\$)				220

Electronic Acknowledgement Receipt	
EFS ID:	6517899
Application Number:	61264120
International Application Number:	
Confirmation Number:	9861
Title of Invention:	DEVICE ASSISTED SERVICES INSTALL
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	21912
Filer:	Michael J. Schallop/Veronica Pula
Filer Authorized By:	Michael J. Schallop
Attorney Docket Number:	RALEP027+
Receipt Date:	24-NOV-2009
Filing Date:	
Time Stamp:	17:32:50
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$220
RAM confirmation Number	4519
Deposit Account	500685
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 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	Provisional Cover Sheet (SB16)	RALEP027plus_Provisional_Coversheet_Efile.pdf	1000036	no	3
			f9e80f8c6a84e0eae3f292fbb8b3986f640148		
Warnings:					
Information:					
2		RALEP027plus_APP.pdf	142600	yes	28
			43e4476022f46da10c8f4b02fc50970611d3b940		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	27	
	Abstract		28	28	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	RALEP027plus_Figures.pdf	537017	no	5
			9a9c8641f3532195be906f21530d4626d846b2b9		
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29099	no	2
			2a011833eddebbcb6faa3fe761b07a21fc2697a9c		
Warnings:					
Information:					
Total Files Size (in bytes):			1708752		

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.