

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
2 December 2010 (02.12.2010)

(10) International Publication Number
WO 2010/138333 A1

(51) International Patent Classification:
H04W 8/18 (2009.01)

(21) International Application Number:
PCT/US2010/035145

(22) International Filing Date:
17 May 2010 (17.05.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/467,282 17 May 2009 (17.05.2009) US

(71) Applicant (for all designated States except US): **QUALCOMM Incorporated** [US/US]; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SANDING, Anthony** [US/US]; 5775 Morehouse Drive, San Diego, Califor-

nia 92121 (US). **VAIDYANATHAN, Balaji** [IN/US]; 5775 Morehouse Drive, San Diego, California 92121 (US). **TUGNAWAT, Yogesh** [IN/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agent: **HAGLER, James T.**; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(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.

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR TRACKING THE PROGRAMMING OF A MOBILE DEVICE WITH MULTIPLE SERVICE ACCOUNTS

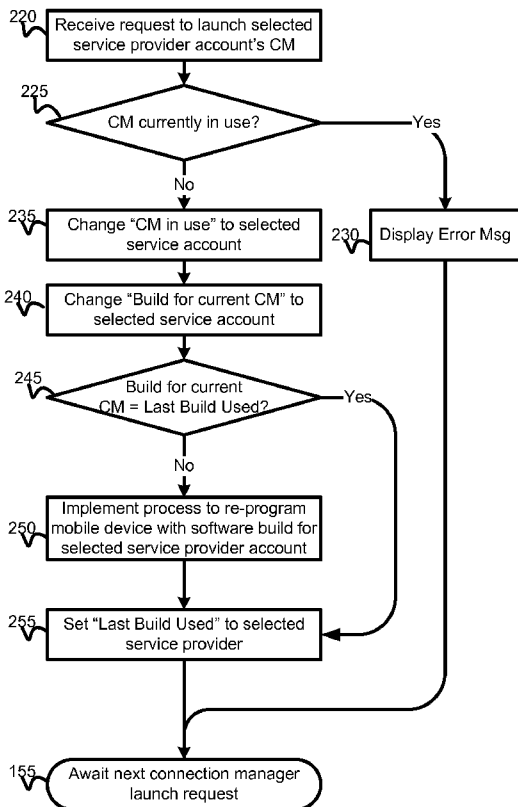


Fig. 15

(57) Abstract: Methods and systems enable mobile devices equipped with software defined radio based chipset modules to seamlessly re-program the mobile device to operate on any of a variety of service provider networks. By re-programming a mobile device equipped with software defined radio based chipset module, the mobile device can support communications over both GSM and CDMA communication networks. The re-programming of the mobile device may commence with the launching of a connection manager supporting a selected service provider. Various embodiment methods and systems are provided to track and monitor a currently activated first connection manager and prevent the launching of a second connection manager while the first connection manager is still active in order to avoid potentially fatal collisions.

WO 2010/138333 A1



(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).

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

Declarations under Rule 4.17:

**METHOD AND APPARATUS FOR TRACKING THE
PROGRAMMING OF A MOBILE DEVICE WITH MULTIPLE
SERVICE ACCOUNTS**

FIELD OF THE INVENTION

[0001] The present invention relates generally to provisioning and programming a mobile device, and more particularly to methods and apparatus for provisioning and programming multiple service provider accounts on a single mobile device.

BACKGROUND

[0002] Typically, conventional cellular communications devices operate using one of two main competing network technologies. Namely, Global System for Mobile Communications (GSM) or Code Division Multiple Access (CDMA). While there are a number of differences between the two competing technologies, at the core GSM implements a time-division multiplexing scheme, while CDMA (as its name implies) implements a code-based multiplexing scheme. In a GSM network a portion of the network's total bandwidth is allocated as a channel to a mobile device. The network base station then selectively "listens" to each of the allocated channels for a short amount of time to send and receive voice and/or data information to and from the mobile device. The base station can only selectively listen to the allocated channel for a short amount of time because it must also listen to other channels allocated to other mobile devices operating on the network. While effective, the TDMA scheme is hampered by its limited bandwidth and need to dedicate a single channel to a single mobile device.

[0003] In contrast, in a CDMA network, each channel may be utilized by multiple mobile devices. In order to differentiate the information received

from different mobile devices operating on the same allocated channel, each mobile device is assigned a different coding offset in which to encode its voice and/or data information. By selectively switching the decoding code offset, the base station can decode the information received from multiple mobile devices operating on the same allocated channel. This greatly increases the capacity to service more mobile devices on the same amount of total bandwidth.

[0004] In addition to the multiplexing and encoding schemes implemented on each of the competing technologies, individual service providers operating competing communication networks may modify other aspects of the communication signals being sent and received over their respective communication networks. This allows each service provider to differentiate their network from another and in some instances offer differentiating features to its customers. These aspects may include communication signal waveforms, frequency, amplitude, etc.

[0005] In order to properly operate on a particular service provider's network, a mobile device must be equipped with the necessary hardware to generate the appropriate waveform with the correct modulation, and coding scheme as required by the service provider's network. Because of the fundamental differences in the type of waveform, modulation and coding schemes used between the two competing networks, mobile devices equipped with the necessary hardware to operate on a GSM technology network cannot operate on a CDMA technology network, and vice versa.

[0006] Moreover, competing service providers operating similar technology (e.g., GSM or CDMA) networks typically implement proprietary provisioning data that allows a mobile device to operate on a particular service provider's network. Each service provider typically employs a number of provisioning parameters that are unique in their usage or format. Conventional mobile devices store the provisioning data for the single service provider with which the device has been registered. While conventional mobile devices may be

able to conduct communications over a different service provider's communication network (provided it is of the same technology type), such usage will be only permitted in accordance with the roaming rules and permissions dictated by the provisioning data loaded into the mobile device. If a user of a conventional mobile device wishes to utilize a different service provider's communication network for primary (i.e., non-roaming) service, the provisioning data loaded into the mobile device must be deleted and replaced with provisioning data of the newly selected service provider. Typically, such a change may only be made by activating a new account with the newly selected service provider. If the user subsequently desires to revert back to the original service provider's communication network for primary service, then a new account on the original service provider's network must be activated and the previous account data deleted.

[0007] In some settings, a removable smart card such as a Subscriber Identity Module (SIM) card or analogous R-UIM card may allow a user to interchange the provisioning data loaded into a mobile device without the need for service provider intervention. The provisioning data for different service providers may be stored on the removable smart card. Because each smart card may store the provisioning data for a different service provider a user may physically interchange smart cards in a mobile device to use different service provider networks for primary service. However, the need to physically interchange smart cards requires a user to carry multiple smart cards. In addition, the physical interchange of smart cards is cumbersome. Lastly, the use of smart cards still does not allow a mobile device equipped with the necessary hardware to operate on a GSM technology network to operate on a CDMA technology network and vice versa.

SUMMARY

[0008] Mobile devices equipped with software based radio chipset modules may be enabled to operate on any of a number of different service providers.

By launching the connection manager for a selected service provider, the mobile device may retrieve the necessary software builds and provisioning data parameters for the selected service provider. Various embodiment methods and systems are provided to track and monitor a currently activated first connection manager and prevent the launching of a second connection manager while the first connection manager is still active in order to avoid potentially fatal collisions.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The accompanying drawings, which are incorporated herein and constitute part of this specification, illustrate exemplary embodiments of the invention, and, together with the general description given above and the detailed description given below, serve to explain features of the invention.

[0010] Fig. 1 is a block diagram depicting typical components of a mobile device capable of supporting the various embodiments.

[0011] Fig. 2 is a hardware/software architecture diagram of software modules operating within a mobile device equipped with a software defined radio based chipset module.

[0012] Fig. 3 is an exemplary data table of dynamic parameters utilized by different service provider accounts.

[0013] Fig. 4 is an exemplary data table of static parameters utilized by different service provider accounts.

[0014] Fig. 5 is an exemplary data table of security parameters utilized by different service provider accounts.

[0015] Fig. 6 is a process flow diagram illustrating example steps which may be implemented to insure that an account for a selected service provider has been activated.

[0016] Fig. 7 is a system diagram of a communication system which allows a mobile device to initiate an activation procedure with a variety of service providers.

[0017] Fig. 8 is a process flow diagram illustrating an embodiment process for seamlessly enabling multiple software builds to support a multiple service provider accounts on the same mobile device.

[0018] Fig. 9 is a process flow diagram illustrating example steps which may be implemented to load the software build for a previously un-activated service provider account.

[0019] Fig. 10 is a process flow diagram illustrating example steps which may be implemented to load the software build for a previously activated service provider account.

[0020] Fig. 11 is a process flow diagram of an alternative embodiment method to confirm an active/valid account with the selected service provider.

[0021] Fig. 12 is a process flow diagram of another alternative embodiment method to confirm an active/valid account with the selected service provider.

[0022] Fig. 13 is a system diagram of an alternative embodiment communication system in which an indexed data table of service provider accounts is stored in a remote non-volatile memory.

[0023] Fig. 14 is a system diagram of another alternative embodiment communication system in which the indexed data table of service provider accounts is stored in a remote non-volatile memory.

[0024] Fig. 15 is a process flow diagram illustrating a process that may be implemented by an exemplary connection manager tracker.

[0025] FIG. 16 is a component block diagram of an example server suitable for use with the various embodiments.

DETAILED DESCRIPTION

[0026] The various embodiments will be described in detail with reference to the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts. References made to particular examples and implementations are for illustrative purposes, and are not intended to limit the scope of the invention or the claims.

[0027] In this description, the term “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any implementation described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other implementations.

[0028] As used herein, the term “mobile device” is intended to encompass any form of programmable computer as may exist or will be developed in the future which implements a communication module for wireless voice and data communications, including, for example, cellular telephones, personal data assistants (PDA's), palm-top computers, laptop and notebook computers, wireless electronic mail receivers (e.g., the Blackberry® and Treo® devices), multimedia Internet enabled cellular telephones (e.g., the iPhone®), and similar personal electronic devices which include a wireless communication module, processor and memory. In a preferred embodiment, the mobile device is a portable computer with a software defined radio based chipset module.

[0029] Conventional mobile devices have typically been designed to operate on a single service provider's communication network. More specifically, conventional mobile devices have been designed to operate on a single communication technology (e.g., GSM v. CDMA). For example, cellular telephones have been typically purchased directly from a service provider for use on that service provider's network. Similarly, wireless modem cards for notebook computers are typically bought and sold directly from the service provider. Because of the fundamental differences between the competing

technologies, the hardware contained within the mobile device enabling communications on one competing technology prevents the same mobile device from communicating with a network of another competing technology.

[0030] Moreover, even as two separate service providers may implement the same communication technology, different service providers may provide their customers with different feature sets. Consequently, even if the hardware enabling communication is the same, the software enabling communications on one service provider's communication network may vary greatly from that of a different service provider. Accordingly, a different software build must be implemented on a mobile device for each service provider.

[0031] In addition, most conventional mobile devices have been designed to load a single service provider's provisioning data. Because competing service providers implement proprietary provisioning data, conventional mobile devices operating on one service provider's communication network cannot operate on another service provider's communication network (as a primary service) without deleting the first service provider's provisioning data and replacing it with the second service provider's provisioning data. While some mobile devices allow a user to exchange the provisioning data of different service providers through the interchange of smart cards, such methods are cumbersome and still do not allow a user to utilize the communication networks of competing technologies.

[0032] In contrast to conventional mobile devices which use hardware to generate, encode/decode, and modulate/demodulate signals in conjunction with one of the competing technologies, future software defined radio based chipset modules, such as Qualcomm's Gobi®, generate, encode/decode and modulate/demodulate data signals within a programmable digital signal processor (DSP). The programmable DSP enables the communication signal to be defined by software to conform with the wave form, frequency and data packet requirements of any communication technology. By re-programming

the DSP to generate signals with different characteristics, the mobile device may be made to generate a communication signal that is compatible with any service provider's unique communications network.

[0033] In order to re-program the DSP within the software defined radio based chipset to generate a data signal compatible with a selected service provider network, the mobile device must load an appropriate software build for the selected service provider. Each service provider's software build may contain the necessary instructions to generate, encode and modulate data signals to be properly carried over the service provider's communication network, as well as contain the necessary programming to carry out all of the additional features offered by the service provider. The various embodiments provide the capability to modify and switch various modules of the software build implemented on a mobile device. Various embodiments monitor which service providers have had an account activated by the mobile device so that previously generated parameters of a service provider's software build may be recycled. Other embodiments monitor the currently implemented service provider software build to prevent fatal collisions from occurring when a different software build is requested.

[0034] Fig. 1 depicts typical components of a mobile device 10 capable of supporting the various embodiments. A typical mobile device 10 includes a processor 191 or dual (or more) processors 191a and 191b coupled to internal memory 192 and a user interface display 11. The mobile device 10 may also include a software-defined communication module 20 which is capable of operating on any of a plurality of service provider communication networks. The software-defined communication module 20 may include non-volatile memory 25 and file systems 26 which may store an indexed table of service provider account parameters and settings for use in modifying the software operation of the device for a selected service provider.

[0035] The mobile device 10 may include an antenna 194 for sending and receiving electromagnetic radiation that is connected to the software-defined communication module 20 coupled to the processor 191. Further, the mobile device 10 includes a speaker 18 to produce audible sound and a microphone 19 for sensing sound, such as receiving the speech of a user. Both the microphone 19 and speaker 18 may be connected to the processor 191 via a vocoder 199 which transforms analog electrical signals received from the microphone 19 into digital codes, and transform digital codes received from the processor 191 into analog electrical signals which the speaker 18 can transform into sound waves. In some implementations, the vocoder 199 may be included as part of the circuitry and programming of the processor 191. Mobile devices also typically include a key pad 13 and menu selection buttons or rocker switches 12 for receiving user inputs.

[0036] The processor 191 may be any programmable microprocessor, microcomputer or multiple processor chip or chips that can be configured by software instructions (applications) to perform a variety of functions, including the functions of the various embodiments described below. In some mobile devices, multiple processors 191 may be provided, such as one processor dedicated to wireless communication functions and one processor dedicated to running other applications. In some mobile devices 10, multiple processors 191a, 191b may be provided to share wireless communication functions and/or application between them. Typically, software applications may be stored in the internal memory 192 before they are accessed and loaded into the processor 191. In some mobile devices, the processor 191 may include internal memory sufficient to store the application software instructions. In some mobile devices the processor 191 is included within the software-defined communication module 20, such as in Qualcomm's Gobi® which includes two processors in addition to signal generator and modem circuits.

[0037] Fig. 2 is a hardware/software architecture diagram of software modules on a mobile device equipped with a software defined radio based chipset

modules. As shown in Fig. 2, the mobile device 10 includes a software defined radio based chipset communication module 20 (communication module), such as Qualcomm's Gobi®. The communication module 20 may optionally contain a non-volatile memory 25 which may store an indexed table of different service provider parameter configurations. In alternative embodiments the indexed data table may also be stored in a remote non-volatile memory (not shown) from which it can be retrieved. An example of the indexed data table is shown in more detail in Fig. 3, below. The various parameters stored in the indexed data table may be used when compiling the particular software build for each service provider supporting an account to which the mobile device has subscribed. Since each service provider may implement a unique software build the parameters for each service provider account often differ from other service provider accounts. In many cases a parameter used in the software build for one service provider may be in a different format or may not be used at all by a different service provider.

[0038] A multi-interface software module 30 functioning in a processor 191 is in communication with the communication module 20 and a common application programming interface (C-API) 40. The multi-interface software module 30 contains the actual coding for various subroutines called on by applications via the C-API 40. Developers of applications for mobile devices 10 can utilize the C-API 40 to access or interface with various subroutine stored in the multi-interface module 30 to perform desired functions. The subroutines stored in the multi-interface module 30 may be used to perform a variety of functions including, but not limited to, programming and retrieving information from the communication module 20. The C-API 40 may contain a number of dynamic link libraries (DLL) 45. By containing a number of dynamic link libraries 45, the C-API 40 may use the hooks to and from the multi-interface module 30 to provision the communication module 20 for a particular service provider. By utilizing dynamically linked libraries of common subroutines, the subroutines appropriate for a selected service

provider may be loaded into an application program at runtime rather than at compile time.

[0039] When an account for a service provider is activated on the mobile device 10, the DLL 45 supporting that account is loaded into the C-API and stored for future retrieval. Each of the various service providers activated on a mobile device 10 may load an application programming interface specific to the particular service provider that uses its respective DLLs to facilitate the loading of the service provider's software build and provisioning data. Each of the DLLs 45 may be programmed to communicate with the multi interface software module 30. The C-API 40 is in communication with a connection manager tracker 50 or directly with a service provider's connection manager. The connection manager tracker 50 effectively acts as a "traffic cop" to insure that only a single service provider's software build is implemented on the mobile device 10 at a time. The connection manager tracker 50 determines which service provider account is selected and insures that only the software build corresponding to the selected service provider account is implemented. In the event a service provider account is selected that is not supported by the currently implemented software build, the connection manager tracker 50 may insure that the currently implemented software build is closed before the software build corresponding to the newly selected service provider account is launched. The connection manager tracker 50 is in communication with each individual connection manager 61, 62, 63 supporting each service provider account (SP1, SP2, SP3) activated on the mobile device 10. Each connection manager 61, 62, 63 is responsible for launching the corresponding software build by loading the appropriate subroutines from the DLLs 45 and retrieving the appropriate parameters stored in non-volatile memory 25.

[0040] In an alternative embodiment, the mobile device 10 may implement a common connection manager 60 which is a central application that is capable of setting up the communication links for a plurality of service provider accounts (SP1, SP2, SP3). In such an embodiment, the connection manager

tracker 50 may be integrated within the common connection manager 60 or may continue to communicate with an external connection manager tracker 50 to insure that only a single service provider's software build is implemented on the mobile device 10 at a time.

[0041] Figs. 3, 4, and 5 illustrate exemplary indexed data tables of dynamic, static and security parameters utilized by a variety of service provider accounts. As shown in Figs. 3, 4, and 5, data associated with service provider accounts may be organized as a table containing a plurality of records (i.e., columns) associated with the service providers, with each record including a plurality of data fields (i.e., rows in Figs. 3, 4, and 5) storing data settings associated with each service provider. The exemplary data table of Figs. 3, 4, and 5 illustrates only 4 service providers (i.e., service provider 1, service provider 2, service provider 3 and service provider 4). However, one of ordinary skill in the art would appreciate that additional columns listing additional service providers may be included. Indeed, a data table may include every service provider operating in the world. Moreover, multiple columns for each service provider may be included in instances where a mobile device 10 maintains multiple accounts on the same service provider's communication network.

[0042] For each service provider, a variety of parameters and settings which are generated during the initial activation process of each respective service provider may be stored in data fields (illustrated as rows in Figs. 3, 4, and 5). Fig. 3 illustrates an exemplary indexed data table of dynamic parameters utilized by a variety of service provider accounts. For example, each service provider may specify a different mode of activation. As the name implies, the mode of activation indicates the type of activation procedure that is employed by the particular service provider. The different types of activation procedures may include, for example, an Over-the-Air Service Provisioning (OTASP) procedure, an Internet Over-the Air (IOTA) procedure, or an Open Mobile Alliance Device Management (OMADM) procedure. Each of these procedures

may implement different steps and/or protocols to accomplish the activation procedure.

[0043] The data table may also specify the Network Access Identifier (NAI) for each service provider. The NAI is the username assigned to the mobile device 10 used to authenticate the device for data service. Each service provider may assign a unique format to the username. For example, service provider 1 uses the service provider 1's name as the domain for each username. Alternatively, service provider 2 utilizes "hcm.SP2.com" as the domain name. In some instances a service provider may assign multiple NAIs to the same mobile device 10. For example, as shown in Fig. 3, Service Provider 2 and Service Provider 4 may assign multiple NAIs to the same mobile device 10. The format of the NAI may differ not only between the different service providers, but also between the various NAIs assigned by the same service provider. Also, as shown in Fig. 3, other service providers such as Service Provider 1 and Service Provider 3 may only assign a single NAI to each mobile device 10. The multiple NAIs may be distinguished by the MIP User Profile N, where $N = \{0, 1, 2, 3, \dots\}$. Thus, while Fig. 3 depicts some service providers assigning two NAIs (i.e., $N = \{0, 1\}$) additional user profiles may be assigned in some instances.

[0044] The data table may further specify the Mobile Node-Home Agent (MN-HA) Shared Secret, also referred to as a password. The MN-HA password may be used to authenticate the mobile device 10 at the Mobile IP Home Agent. Each service provider may assign a unique format to the username. For example, service provider 3 uses the first 16 digits of the Authentication Key (Akey), while service provider 4 uses an 8 character Psuedo ESN (pESN). As a further example, service provider 2 utilizes "hcm.SP2.com" as the domain name. Similar to the NAI, service providers may assign multiple MN-HA passwords to the same mobile device 10, such as shown in Fig. 3 for Service Provider 2 and Service Provider 4. Also, as shown in Fig. 3, other service

providers such as Service Provider 1 and Service Provider 3 may only assign a single MH-NA password to each mobile device 10.

[0045] The data table may further specify the Mobile Node-Authentication, Authorization, and Accounting (MN-AAA) Shared Secret (password) which authenticates the mobile device 10 to the billing server (not shown). Again, each service provider may use a different specific format. Additionally, each service provider may utilize different values for each entry. Similar to the MN-HA password and NAIs, service providers may elect to assign multiple MN-AAA passwords to each mobile device 10.

[0046] In addition, the data table may specify other parameters and settings such as the Simple IP Authentication, Authorization, and Accounting NAI (SIP AAA NAI), which is sometimes referred to as the Simple IP Username. The data table may further specify the Simple IP Authentication, Authorization, and Accounting Password (SIP AAA password) which is a Simple IP password. Other parameters may include the Simple Parameter Index (SPI), not shown. It is noted that not all types of parameters and settings are used by all service providers. For example, while service providers 2 and 4 utilize a parameter for MN-HA Shared Secret – Slot 1, service providers 1 and 3 do not utilize such a parameter. For some service providers no value may be recorded in the indexed data table for such a non-utilized parameter. In other cases, a null value may be stored as a place holder for such a value.

[0047] Fig. 4 illustrates additional example data entries in the exemplary indexed data table beyond those shown in Fig. 3. For example, each service provider may specify a different mobile node authenticator (MN Authenticator). In the example shown in Fig. 4, only service provider 1 requires a value for this parameter. The data table of Fig. 4 also shows various formats or values specified by service providers for the Mobile Node Home Address SPI Set (MN HA SPI Set), MN HA SPI Value, MN AAA SPI Set, MN AAA SPI Value, Reverse Tunneling, QNC Enabled, Home Address, Primary

HA Address, Secondary HA Address, Initial Registrations Retry Interval Time, Registry Retry Number, DS MIP De-registrations Retries, and Pre-Lifetime-expiry Re-Registration time.

[0048] Fig. 5 illustrates additional example data entries in the exemplary indexed data table beyond those shown in Figs. 3 and 4. The data table of Fig. 5 also shows example formats or values that service providers may use for SPC, One Time Keypad Subsidy Lock (OTKSL), Number of Incorrect Service Programming Code (SPC) Attempts, Field Service Code, Akey Checksum, simple message service (SMS) support.

[0049] The parameters and settings listed in the indexed data tables shown in Figs. 3, 4, and 5 are intended to be illustrative only and provide examples of possible formats and values utilized and implemented by different service providers. One of skill in the art would appreciate that service providers may employ several other parameters and settings utilized in their various software builds which may be reflected in the indexed data table.

[0050] When a user elects to initiate communications on a mobile device 10, the user may select a service provider account to support the communication by launching a connection manager (e.g., 60, 61, 62, 63) corresponding to the selected service provider account. In instances where the mobile device 10 is a cellular telephone, a service provider account is typically running at all times. However, in instances where the mobile device 10 is a wireless modem card within a notebook computer, a service provider account is typically not running unless communication capabilities are desired. In order to initiate communications, the user may launch a service provider's independent connection manager. Alternatively, the user may select a particular service provider from a choice of several service providers presented in a user interface display generated by a common connection manager. A similar menu may be provided on a cellular telephone to select a new service provider account which would be analogous to launching a connection manager on a notebook

computer. By launching the connection manager (60, 61, 62, 63) corresponding to the desired service provider account, the connection manager (60, 61, 62, 63) communicates with the C-API 40, either directly or through a connection manager tracker 50, to call up each of the necessary subroutines contained in the DLL 45 necessary to complete the software build necessary for communications over the selected service provider network. In addition, the C-API 40 may access the DLL 45 to retrieve the necessary parameters stored in a non-volatile memory 25 and/or File System 26 via multi-interface module 30. The necessary parameters are stored in an indexed data table. That data table may contain each of the assigned parameters for a selected service provider account that have been previously generated during an initial service provider account activation procedure.

[0051] Referring back to Fig. 2, in some instances a mobile device 10 may be loaded with a variety of connection managers (61, 62, 63) as part of an original equipment manufacturer's (OEM) software package. These connection managers (61, 62, 63) may be individual connection managers loaded on the mobile device or may be possible selections on a common connection manager program 60. In such instances, it is likely that a user has not established a service provider account with any/all of the service providers corresponding to each of the connection managers/selections. Therefore, the mobile device 10 may be provisioned with the default parameters as prescribed by the selected service provider only. Consequently, when a user launches a connection manager for a service provider that does not have a service provider account associated for the mobile device 10, an error will occur since the necessary parameters of a valid subscription will not be stored in the indexed data table. Accordingly, each time a connection manager/selection is launched, a test to determine whether an account has been activated for the selected service provider may be performed.

[0052] Fig. 6 illustrates a process that may be implemented on a mobile device 10 each time a connection manager is launched to determine if an account on

the selected service provider has been activated. When a user attempts to launch a connection manager for a selected service provider, the request is received by the processor 191, step 101. Upon receipt of a request to launch a connection manager for a selected service provider, the processor 191 may determine whether an account has previously been activated for the selected service provider, decision 105. This determination process may be accomplished by checking the status of an activation flag associated with each service provider. Alternatively, this determination may be accomplished by checking the parameter values stored in the indexed data table (see Figs. 3-5) for the selected service provider. If the parameter values stored in the indexed data table are either absent or default values, it may be assumed that an activation procedure has not been completed. If the processor 191 determines that an account has been previously activated on the mobile device 10 (i.e., decision 105 = Yes), then the processor 191 retrieves the parameter values stored in the indexed data table and implements these values while loading or compiling the software build corresponding to the selected service provider, step 110. If an account has been activated, then the selected connection manager may proceed to request the C-API 40 to call up the necessary subroutines in multi-interface module 30 via the DLL 45 and retrieve the stored parameters from the indexed data table in non-volatile memory 25 and/or file systems 26 to implement the appropriate software build.

[0053] If, however, the processor 191 determines that an account for the selected service provider has not been previously activated (i.e., decision 105 = No), then the processor initiates the appropriate activation procedure in order to obtain all of the necessary software build parameters for the selected service provider, step 115. Once these parameter values have been obtained and stored to the indexed data table, an activation flag indicating that an account has been activated on the selected service provider may be optionally set, step 120.

[0054] When a mobile device 10 initially activates an account with a selected service provider, the type of activation procedure that is initiated will depend

upon the selected service provider. Thus, the type of activation procedure required for each individual service provider may also be stored in the indexed data table. For example, some service providers may require that the mobile device 10 initiate an Over-the-Air Service Provisioning (OTASP) procedure, an Internet Over-the Air (IOTA) procedure, or an Open Mobile Alliance Device Management (OMADM) procedure.

[0055] In an OTASP procedure, the mobile device 10 may be directed to wirelessly call a specified number (e.g., *228). While the mobile device 10 may not have sufficient parameter data to conduct unlimited communications on a service provider's network, the mobile device 10 may be programmed by the OEM with sufficient parameter data to conduct limited communications to contact a selected service provider's activation server for initial activation purposes. Once connected to the service provider's activation server the mobile device 10 receives various parameter and settings from the service provider's activation server which are used to configure the appropriate software build on the mobile device 10. Some of the parameters and settings may include a mobile identification number (MIN), preferred roaming list (PRL), as well as mobile directory number (MDN) and mobile station identifiers (MSID) both of which may be referred to as the mobile device's phone number. Once the OTASP procedure is complete, the mobile device 10 may be required to initiate an authentication parameters generation procedure which authenticates the mobile device 10 to the service provider by generating usernames and/or passwords. Similarly, in an IOTA procedure, the mobile device may receive parameters and setting such as a MIN and MSID. However, rather than performing a separate authentication process, the IOTA process also generates and assigns passwords and usernames to the mobile device 10. Once either activation process is complete, the parameters and settings received during the activation procedure may be stored in the indexed data table in a non-volatile memory 25.

[0056] Fig. 7 illustrates an exemplary communication system which allows a mobile device 10 to initiate an activation procedure with a variety of service providers. Fig. 7 includes two service providers 125, 130 for illustrative purposes; a multitude of service providers may be included in the embodiment communication system. To initiate an activation procedure with a service provider wirelessly, the mobile device 10 must have sufficient software and provisioning data to access the service provider's communication network 100, 102 and connect with an activation server 125a, 130a. Accordingly, OEMs may load sufficient software and provisioning data to enable a mobile device to contact one or many service providers' activation server 125a, 130a. The activation servers 125a, 130a may be accessed by dialing a special numbers (e.g., *228) to initiate an OTASP/IOTA/OMADM procedure.

[0057] Alternatively, if the necessary minimum software and provisioning data is not loaded onto the mobile device 10 by the OEM, the mobile device 10 may connect through specified telephone numbers or website URLs maintained by a service provider's activation server 125a, 130a via wired connections through a wired communication network 104 to initiate activation procedures. Once connected to the service provider's activation server 125a, 130a the mobile device 10 may be connected through a mobile switching center 125b, 130b to the service provider's provisioning server 125c, 130c. As part of an activation process, the mobile device's 10 unique serial number, (e.g., mobile equipment identifier (MEID) and international mobile equipment identifier (IMEI)), may be transmitted to the service provider's provisioning server 125c, 130c for association with an account with the selected service provider. In return the service provider provisioning server 125c, 130c may transmit various parameters and settings necessary to operate on the service provider network. Alternatively, the service provider provisioning system may communicate with an external server to obtain the parameters or vice-versa. Such parameters and settings may be stored in the indexed data table in the non-volatile memory 25.

In addition, a DLL 45 containing necessary subroutines for the selected service provider's software build may be transmitted to the mobile device 10.

[0058] Once the mobile device 10 has received all of the necessary parameters, settings and DLL 45 from the service provider provisioning server 125c, 130c, a connection manager for the selected service provider may be launched in the mobile device's processor 191. In case of modules embedded in computers or add-on cards, the connection manager may be launched in the computer in which the module is embedded or to which the module is connected. As discussed above, the launched connection manager may point to the corresponding software build file in memory. The software build file may contain all of the necessary instructions and subroutines required to compile the completed software build. The software build file may recall the necessary subroutines found in the DLL 45 and parameters associated with the selected service provider found in the indexed data table which is stored in a non-volatile memory 25 to modify the behavior of the appropriate software build to conduct communications over the selected service provider's communications network.

[0059] Fig. 8 is a process flow diagram of embodiment steps for re-programming the mobile device 10 with a different software build to change service provider accounts. When a user elects to initiate communications on a mobile device 10, the user may select a service provider account to support the communication by launching a connection manager (e.g., 61, 62, 63) corresponding to the selected service provider account. In instances where the mobile device 10 is a wireless telephone, a service provider account is typically running at all times. Thus, a menu may be presented on a user interface display to prompt the user to select a new service provider. In a response to the menu display, the processor 191 may receive a request from the user to switch to a new service provider account, step 101. For example, a request to switch to a new service provider account may be received when a new connection manager is launched by a user action or a different service provider is selected by a user

from a common connection manager. The processor 191 may optionally present a display requesting the user to confirm that the user intends to switch service provider (SP) accounts, decision 131. By confirming the user's intention, unwanted or unintentional changes to the software build currently implemented on the mobile device 10 may be avoided

[0060] If the user responds to the inquiry in the negative (i.e., decision 131 = No), then the processor 191 closes the launched connection manager (61, 62, 63) or deselects the connection manager from the common connection manager 60, step 135. Once the connection manager is closed or deselected, the processor 191 may await the next connection manager launch request or selection of a different service provider step 155.

[0061] If the user confirms an intention to switch service provider accounts (i.e., decision 131 = Yes), the processor 191 determines if an account with the selected service provider has been previously activated, decision 140. In an embodiment, a flag may be set in memory if an account has been previously activated on a selected service provider. This flag may be separately recorded in an indexed data table of service provider software parameters. Other indicators beside a flag may be used to indicate whether an account with the selected service provider has been previously activated. For example, in an alternative embodiment the processor 191 may check the format of the mobile identification number (MIN) stored in the indexed data table of service provider software parameters. The MIN is a 10-digit number unique to each mobile device which a service provider uses to identify individual mobile devices. Typically, after an account is activated with a service provider the MINs format will be altered from its original manufacturer format of 000-000-WXYZ. If the original manufacturer format exists, then no previous account has been activated on the mobile device 10.

[0062] If an account with the selected service provider has not been previously activated (i.e., decision 140 = No), then the processor 191 loads the software

build for the un-activated selected service provider, step 145. Once the software build is loaded, the mobile device 10 may attempt activation on the selected but previously un-activated service provider network. If the activation was successful (i.e., decision 146 = Yes), then a flag may be set indicating that an account with the selected service provider has been activated, step 150. After setting the flag indicating that an account with the selected service provider has been activated, a call may proceed and the processor 191 may await the next connection manager launch request or selection of a different service provider, step 155. If the activation in step 145 was not successful (i.e., decision 146 = No), then the processor 191 may repeat step 145 (see also process flow diagram illustrated in Fig. 9) in an attempt to successfully activate an account for the selected but previously un-activated service provider. In an alternative embodiment, the processor 191 may inform user of the failed activation attempt and inquire whether the user wishes to repeat the activation attempt, step 147. If the user elects to continue activation attempts (i.e., decision 147 = Yes), then the processor repeats step 145 (see also process flow diagram illustrated in Fig. 9) in an attempt to successfully activate an account for the selected but previously un-activated service provider. However, if the user elects to cancel the activation attempt (i.e., decision 147 = No), then the processor 191 may await the next connection manager launch, or selection of a different service provider, step 155.

[0063] In an alternative embodiment where the processor 191 may check the format of the mobile identification number (MIN) stored in the indexed data table of service provider software parameters to determined whether an account has been previously activated (i.e., decision 140), the MIN's format will have already been altered from the original manufacturer format during the software build load step 145. Accordingly, step 150 will not be necessary.

[0064] If the processor 191 determines that an account with the selected service provider has been previously activated (i.e., decision 140 = Yes), then the processor 191 may load the selected service provider's software build, step

160. Once the software build is loaded, the processor 191 retrieves from non-volatile memory the various parameters and settings previously stored in the indexed data table of service provider accounts, step 165. In some instances it may be the case that while an account was previously activated on the mobile device 10 for the selected service provider, the activated service provider account may have lapsed or been abandoned. This may occur, for example, when trial subscriptions for service are offered or a user temporarily elects to no longer utilize the selected service provider to support calls. Accordingly, it may be necessary to confirm that an account is still active/valid for the selected service provider.

[0065] In an embodiment, the processor 191 may request the user to confirm that a prior account on the selected service provider was previously active and that the user wishes to switch to this previously activated account, decision 170. If the user confirms that a prior account on the selected service provider was previously active and that the user wishes to switch to this previously activated account (i.e., decision 170 = Yes), the processor 191 implements the selected service provider account to support its data calls and awaits the next connection manager launch request or selection of a different service provider, step 155.

[0066] In some instances a user may have previously activated an account with the selected service provider, but has either intentionally or unintentionally abandoned the previously activated service provider account. Thus, in the case of intentional abandonment, the user may indicate that a previously activated service provider account is no longer active (i.e., decision 170 = No).

Alternatively, in the case of unintentional abandonment, the user may simply not know whether an account on the selected service provider account is active. Therefore, if the user does not confirm a desire to switch to the previously activated account (i.e., decision 170 = No), the processor 191 completes a process of loading a software build for a previously un-activated service provider. Since many service providers expect a mobile device 10 to be used

with a single service provider, some service provider software builds expect the mobile device 10 to be set to its original factory default settings and parameter values. Therefore, the processor 191 may reset the mobile device 10 to its original factory default setting and parameter values, step 175. Once the mobile device 10 has been reset to the original factory default settings and parameter values, the processor 191 resets the flag used in decision 140 indicating previous activation with the selected service provider, step 176, so that the activation status for the selected service provider is cleared when the account active status is undetermined (i.e., an account with the selected service provider has been activated (decision 140 = Yes), but the user has failed to confirm activation (decision 170 = No)). Resetting the flag indicating that an account with the selected service provider has been previously activated will require the user to activate an account with the selected service provider the next time the service provider is selected. This is because the next time the processor reaches decision 140 the reset flag will create a No output. One of skill in the art may appreciate that the end user may have to contact customer service of the selected service provider for activation/reactivation, if needed.

[0067] In an alternative embodiment where the processor 191 checks the format of the mobile identification number (MIN) stored in the indexed data table of service provider software parameters step 176 may be unnecessary as such embodiments do not utilize such a flag. In addition, since step 175 previously reset the mobile device to its original factory settings and defaults the MIN entry for the selected service provider stored in the indexed data table will reset back to its original manufacturer format of 000-000-WXYZ. Consequently, in the alternative embodiment the user will be required to activate an account with the selected service provider the next time the service provider is selected.

[0068] Once the software build is loaded and the factory default parameters are reset (step 175) and the any necessary resetting of flags, deletion of data or resetting of MIN (step 176), the processor 191 implements the selected service

provider account to support its data calls and awaits the next connection manager launch request or selection of a different service provider, step 155.

[0069] Alternative embodiments for confirming whether an account for the selected service provider is currently active and capable of supporting calls are described in more detail below with respect to Figs. 11 and 12.

[0070] Fig. 9 is a process flow diagram illustrating example steps which may be implemented to load the software build for a previously un-activated service provider account (step 145 in Fig. 8). Once a particular service provider is selected (step 101 of Fig. 8), the processor 191 implements the necessary APIs and DLLs for the selected service provider, step 201. As a mobile device 10 performs an activation procedure with various service providers to set up an account, the software builds associated with each service provider may be stored in memory for subsequent retrieval. The software builds may be setup in directories such that the processor may quickly locate the appropriate software build file for quick and efficient retrieval. For example, each new build may be stored in the mobile device memory 192 with a filename that differs from one another by service provider name and/or account name. Because the stored software builds are for previously un-activated service provider accounts, all of the parameters and settings stored with the software builds are default parameters and settings. These default parameters and settings should be in accordance to service providers' requirements. The default parameters and settings may be updated during the activation process. In addition when the processor implements the necessary APIs and DLLs for the selected service provider (step 201), the processor 191 may also perform additional procedures specific to each service provider to ensure that the software build and parameters are successfully loaded into the device.

[0071] Once the new software build has been located and retrieved, the download service is reset, step 202. In an embodiment, the download service reset process may be a Windows® service restart. The download service may

be stopped and restarted by an API call. The download service may read a configuration file. The configuration file may contain the path to the software build for a particular service provider, and other files needed by the mobile device 10 to operate on that service provider's network. The download service may read this configuration file on restart. Accordingly, the download service may be required to be reset/restarted (step 202) so that the new changes in the configuration file may take effect.

[0072] Next the necessary files may be written into or deleted from the extended file service (EFS), step 204. The necessary files may be stored in the multi-interface module 30 during initial production of the mobile device 10, incorporated into the software build package, incorporated in a connection manager tracker application, or incorporated into a common connection manager installation package. As the software build for each new service provider account is loaded, the EFS files of the previously selected service provider account are deleted or replaced with those of the newly selected service provider account. Once the necessary files are written into or deleted from the EFS, the mobile device 10 may be reset so that the new changes take effect, step 205. With the mobile device 10 reset, the activation process for the selected service provider is initiated so that the appropriate parameters and settings may be obtained to complete the implementation of the software build, step 206. One of skill in the art would appreciate that in some instances a service call to a technician or operator for the selected service provider may be required to initiate the activation process. Once the activation process is complete, the mobile device 10 is capable of supporting communication over the newly selected service provider's network.

[0073] Fig. 10 is a process flow diagram illustrating example steps which may be implemented to load the software build for a previously activated service provider account (step 160 in Fig. 8). The process to load the appropriate software build for a previously activated service provider account is similar to the process for loading an appropriate software build for a previously un-

activated service provider account. Once a particular service provider is selected (step 101 of Fig. 8), the processor 191 implements the necessary APIs and DLLs for the selected service provider, step 201. The processor 191 may also perform additional procedures specific to each service provider to ensure that the software build and parameters are successfully loaded into the device. Once the new software build has been located and retrieved, the download service is reset, step 202. In an embodiment, the download service reset process may be a Windows® service restart. The download service may be stopped and restarted by an API call. The download service may read a configuration file. The configuration file may contain the path to the software build for a particular service provider, and other files needed by the mobile device 10 to operate on that service provider's network. The download service may read this configuration file on restart. Accordingly, the download service may be required to be reset/restarted (step 202) so that the new changes in the configuration file may take effect. Once the download service has been reset (step 202), the processor 191 writes into or deletes from the EFS all necessary files for the pointed software build. Once the necessary files are written into or deleted from the EFS, the mobile device 10 is reset so that the new changes take effect, step 205. With the mobile device 10 reset, the mobile device 10 is capable of supporting communication over the newly selected service provider's network. In contrast to the process flow shown in Fig. 9 and described above, since the mobile device 10 has previously activated an account with the selected service provider there is no need to initiate the activation process for the selected service provider (step 206).

[0074] In many instances, when asked, a user may incorrectly confirm the prior activation of the selected service provider account (i.e., decision 170 = Yes). Put another way, many users may not accurately know the status of each possible service provider account previously activated on their mobile device 10. For example, a user may have knowingly or unknowingly activated a trial subscription with a particular service provider. In either instance, the user may

not know that the trial subscription has expired, but the parameters in the mobile device 10 will have been altered to indicate prior activation with the selected service provider despite the absence of an active/valid service provider account to support calls on the selected service provider's network.

Consequently, when the mobile device 10 performs the process flow shown in Fig. 8, the mobile device 10 will attempt to load the software build for the previously activated service provider, but no call will be supported by the selected service provider's network because there is no active/valid account to support the call. This may lead to an unpleasant user experience and frustration by the user to initiate or receive a call through the selected service provider network.

[0075] Although the use of an optional flag set and stored in memory to indicate whether an account with the selected service provider has been previously activated may be implemented, such flags may be unreliable to indicate whether an account with the service provider is still active/valid. This is particularly the case where a previously activated account has not been explicitly abandoned or lapsed. Accordingly, other alternative embodiments may be necessary to confirm whether an account with the selected service provider has been activated and is still active/valid.

[0076] Fig. 11 is a process flow diagram of steps that may be implemented to automatically confirm and/or create an active account on with the selected service provider. The steps shown in the process flow of Fig. 11 may be performed to derive the decision of decision 170 in Fig. 8. The process flow begins by initializing a "Failure to Connect" counter by setting the counter to zero, step 260. The mobile device 10 may then attempt to make a data call, step 261, and determine whether the data call was successful or failed, decision 262, where "fail" is an authentication failure. The most common form of failure may be a Windows Dial-Up Network Connection (DUNC) error 691. If the call did not fail (i.e., decision 262 = No), then the service provider account is deemed to be valid, step 263, and calls may be accordingly supported by the

selected service provider network using the active/valid account. Thus, the processor may move onto step 155 to await the next connection manager launch request or selection of a different service provider.

[0077] However, if the data call is deemed to have failed (i.e., decision 262 = Yes), then the processor 191 may determine if the mobile device 10 is currently within range of the selected service provider's home system, decision 265. If the mobile device 10 is not currently within range of the selected service provider's home system (i.e., decision 265 = No), the processor 191 may presume that the mobile device 10 is in a roaming state and may indicate the roaming condition to the user. Since many if not all service providers do not support roaming data calls, the mobile device's 10 roaming condition may prevent the data call from being successful. Thus, explaining the reason for the failed call attempt. The user may have to either wait until the mobile device 10 is moved within range of the selected service provider's home system or select a different service provider to support the call. Once the roaming condition is indicated to the user, the processor 191 may move onto step 155 to await the next connection manager launch request or selection of a different service provider.

[0078] Assuming an active/valid account on the selected service provider, the attempted call should be successful provided the mobile device 10 is within the range of the selected service provider's home system. Therefore, if the processor determines that the mobile device 10 is in range of the selected service provider's home system (i.e., decision 265 = Yes), but the data call failed (i.e., decision 262 = Yes), the processor 191 may increment the FTC counter, step 267, and determine if the FTC counter is equal to some predetermined value "X", decision 268. The value of X is arbitrary and may be selected such that the number of attempts to make a data call does not exceed an unreasonable number. If the FTC counter does not equal X (i.e., decision 268 = No), the processor 191 may attempt to make another data call, step 261.

[0079] However, if the FTC counter does equal X (i.e., decision 268 = Yes), meaning the number of attempts equals the “not to exceed” value then it is likely that the service provider account corresponding to the loaded software build is no longer active. Therefore, a new service provider account should be activated. Accordingly, when the FTC counter equals X (i.e., decision 268 = Yes) then the factory default parameters may be reset as in step 175 of FIG. 8. Subsequently, the process flow shown in FIG. 8 (i.e., steps 176 and 155) may be implemented to load and activate a software build for the selected service provider.

[0080] Fig. 12 is a process flow diagram of an alternative embodiment method to confirm an active/valid account with the selected service provider. The method illustrated in Fig. 12 is similar to the method shown in Fig. 11 and performs steps 260-268 in the same manner as described above with reference to Fig. 11. However, in Fig. 12 when the FTC counter equals the arbitrary value “X” (i.e., decision 268=Yes), the processor 191 changes the credentials (MIN, MDN, MIP Profile, Passwords etc) stored in the memory 25 or file system 26 to “boot strap” credentials, step 280. The boot strap credentials are known working credential values for each known service provider. The boot strap credentials for each known service provider may be loaded into the mobile device’s EFS by an OEM or during mobile device initialization. The boot strap credentials for the selected service provider are retrieved from EFS and written into the non-volatile memory.

[0081] In addition, the credential values/settings (actual password) currently existing in the mobile device’s non-volatile memory are stored in a temporary file created in EFS. By changing the credential values stored in non-volatile memory to the boot strap values for the selected service provider, the mobile device can be assured to have known working credential values stored in non-volatile memory that will allow the mobile device to complete a data call to at least an accounts server 180 (discussed in more detail below with reference to Figs. 13 and 14). Once the accounts server 180 is contacted, information

regarding all active accounts supporting the mobile device 10 may be determined.

[0082] While changing the credential values stored in non-volatile memory will allow a call to at least the accounts server 180, a routine will be required to repair the settings in the mobile device. In the embodiment process flow shown in Fig. 12, as part of the process to change the mobile device's credentials, the processor 191 may create a copy of all the existing credentials. Once the processor 191 has created a copy of all the existing credentials, the processor 191 may direct the mobile device 10 to connect to the accounts server 180 (see Figs. 13 and 14), step 281. The accounts server 180 may be in connection with each service provider's Operator Home Location Register/Authentication, Authorization, and Accounting (HLR/AAA) server (not shown). By connecting to the selected service provider's Operator HLR/AAA server, the accounts server 180 may determine if an account on the selected service provider is active/valid for the mobile device 10 in question, decision 282. If an account with the selected service provider is active (i.e., decision 282 = Yes), then the processor 191 may check the previously existing credentials which have been copied and stored in a temporary file in the EFS with the credential values stored for the selected service provider account in the selected service provider's HLR/AAA to determine a match, decision 283. Any distinctions between the credentials stored in the temporary file and those stored for the selected service provider account in the selected service provider's HLR/AAA may be the cause for the failed data call attempt. If the credentials stored in the temporary file in the EFS match those stored in the selected service provider's HLR/AAA server (i.e., decision 283 = Yes), then it is likely that another some temporary external interference or cause exists for the failed data call attempt. Accordingly, the selected service provider account will likely be able to support a data call after some passage of time or movement of the mobile device. Consequently, the processor may move to step 155 to await the next connection manager launch request or selection of a

different service provider. If however, a discrepancy between the credentials stored in the temporary file in the EFS and those stored in the selected service provider's HLR/AAA server exists (i.e., decision 283 = No), then the credentials stored in the selected service provider's HLR/AAA server may be written into the non-volatile memory of the mobile device 10, step 284. After the credentials stored in the mobile device's non-volatile memory are updated to those credential values stored in the selected service provider's HLR/AAA server, the processor 191 may return to step 155 to await the next connection manager launch request or selection of a different service provider.

[0083] In other alternative embodiments (not shown), other repair routines may be implemented which involve network initiated sessions for known activation methods such as OTAPA or Network Initiated IOTA to correct the mobile device credentials. Such alternative embodiment repair routines may also involve asking the end-user to perform known end-user initiated activation methods to repair issues with the mobile device. One of skill in the art would appreciate that various provisions in OTASP, OTAPA, IOTA and OMADM allow specific parameters to be written to the mobile device which may repair the mobile device and subsequently allow proper usage.

[0084] However, if an account with the selected service provider has not been previously activated (i.e., decision 282 = No), then it is likely that the service provider account corresponding to the loaded software build is no longer active. Therefore, a new service provider account should be activated. Accordingly, if the selected service provider account is not active (i.e., decision 282 = No) then the factory default parameters may be reset as in step 175 of FIG. 8. Subsequently, the process flow shown in FIG. 8 (i.e., steps 176 and 155) may be implemented to load and activate a software build for the selected service provider

[0085] The indexed data table of service provider accounts may be stored in a non-volatile memory 25 contained within the communication module 20 for

retrieval by the processor 191. In an alternative embodiment, the contents of the non-volatile memory may be remotely located. Fig. 13 illustrates an embodiment system wherein the indexed data table of service provider accounts may be stored in a remote data server. As described above with reference to Fig. 7, a mobile device 10 may communicate with a plurality of service providers 125, 130 to receive the necessary parameters, settings and provisioning data via communication networks 100, 102. Alternatively, if the necessary minimum software and provisioning data is not loaded onto the mobile device 10 by the OEM, the mobile device 10 may connect through specified telephone numbers or website URLs maintained by a service provider's home address server 125, 130 via wired connections through a wired communication network 104 to initiate activation procedures.

[0086] Referring to Fig. 13, the mobile device 10 may transmit the received data to an account server 180 for storage in an account database 185 in communication with an account server 180 or a non-volatile memory unit within the account server 180 via the communication networks 100, 102 or Internet 104. Each of the various parameters, settings and provisioning data received from the service provider (125, 130) may be stored for each individual mobile device 10 in communication with the account server 180. For example, the account database 185 or non-volatile memory unit within the account server 180 may store an account data table which may be an indexed accounts data table for all mobile devices serviced by the account server 180. Each individual mobile device may be identified in the indexed accounts data table by the mobile device's phone number, unique serial number (such as mobile equipment identifier (MEID) or international mobile equipment identifier (IMEI)) or some other designation such as a generated account name, or user customized account name. For each mobile device entry in the indexed accounts data table, an indexed data table record such as illustrated in Figs. 3-5 may be stored. In this manner, the account server 180 maintains a record of the various parameters, settings and provisioning data that a particular mobile

device 10 serviced by the account server 180 has previously generated. By storing the parameters, settings and provisioning data in a remote database, the local memory requirements of the mobile device 10 may be dramatically reduced. In addition, the remote storage of the parameter, setting and provisioning data may provide a degree of security to prevent unfettered access to a user's parameters, setting, and provisioning data in the event the mobile device 10 is stolen or inappropriately acquired. This is also useful for cases when a user voluntarily replaces the mobile device 10. The transfer of service provider accounts data to the new mobile device 10 is easier to accomplish with remotely stored credentials.

[0087] Fig. 14 illustrates another alternative embodiment system wherein the indexed data table of service provider accounts is stored in a remote server location. As each software defined radio based chipset module is manufactured, it is assigned a unique serial number (MEID or IMEI) by the manufacturer. Typically, the manufacturer maintains a listing of these serial numbers in a manufacturer server 190 or in an accompanying database (not shown separately). An accounts server 180 may be in communication with the manufacturer server 190 to obtain the listing of the manufactured software based radio chipsets serial numbers. These serial numbers in the listing may be used to identify individual mobile devices in an indexed accounts data table. The communication link between the accounts server 180 and the manufacturer server 190 may be via a hardwired direct link, via the Internet 104, or via a wireless communication link 100, 102. When a mobile device 10 launches an initialization procedure with a service provider 125, 130, the mobile device's unique serial number may be sent to the service provider 125, 130 so that the service provider may monitor network usage of each individual mobile device 10. In return the selected service provider 125, 130 may transmit the necessary parameters, settings and provisioning data to the mobile device 10. Alternatively or in addition, the parameters, settings and provisioning data transmitted to the mobile device 10 may be transmitted to the accounts server

180 for remote storage in an indexed data table. The accounts server 180 may store the parameters, settings, and provisioning data in an indexed accounts data table record for each mobile device 10 serviced by the account server 180. By storing the parameters, settings and provisioning data in a remote database, the local memory requirements of the mobile device 10 may be dramatically reduced. In addition, the remote storage of the parameters, settings and provisioning data may provide a degree of security to prevent unfettered access to a user's parameters, settings, and provisioning data in the event the mobile device 10 is stolen or inappropriately acquired. Further, in embodiments where the parameters, settings and provisioning data are sent directly to the accounts server 180 and then subsequently downloaded to the mobile device 10 as needed, processing power and battery life may be conserved. In addition, by storing each of the various parameters, settings and provisioning data for each of the service provider accounts activated by the mobile device 10 in a central location, a processor may quickly and efficiently keep track of which service providers have been activated on a particular mobile device 10.

[0088] As previously discussed, it may be important for a mobile device 10 to track which connection manager is currently operating and to insure that a subsequent connection manager is not launched until the currently operating connection manager is closed. This is because the launching of a subsequent connection manager while a current connection manager is currently operating may cause fatal collisions and a shutdown of the mobile device processor 191. Accordingly, a connection manager tracker 50 may be included to provide the necessary process to insure that two connection managers are not simultaneously launched on the same processor 191. Thus, each time a connection manager is launched, a flag indicating that a connection manager is active may be set in memory. In addition, the name of the currently launched connection manager may be stored in memory or a buffer. Each time the processor 191 receives a request to launch a connection manager, the processor 191 may first check the connection manager active flag to determine if it is set.

If it is not set, then no connection manager is currently active. Therefore, the new connection manager may be launched without incident. However, if the connection manager active flag is set, the processor 191 may check to see which connection manager is currently active. If the currently active connection manager differs from the connection manager selected by the user for launch, then the processor 191 must deactivate the currently active connection manager prior to launching the selected connection manager. Such a connection manager tracker process may be used in embodiments where an independent connection manager exists for each service provider account or in embodiments where a common connection manager 60 allows a user to select a particular service provider account from a plurality of possible selections.

[0089] As previously discussed, at any time a processor 191 may receive a request from a user to launch a connection manager supporting a particular service provider account. For example, if the mobile device 10 is a cellular telephone, where communications are typically always active, the request to launch a connection manager would be in response to a user seeking to change the service provider account currently supporting communications. In other instances, such as when the mobile device 10 is a notebook computer with a wireless modem, communications capabilities are not always activated. Thus, the launching of a connection manager may indicate that the user wishes to enable wireless communications capability of the notebook computer. To prevent conflicting instructions to the software defined radio based chipset module 20, a currently enabled connection manager should be deactivated before a new connection manager is activated. If two different connection managers are concurrently activated, the possible conflicting software builds (e.g., a GSM software build and a CDMA software build) may cause errors in the software defined radio based chipset module 20. Accordingly, a process to track and control which connection manager is currently activated may be desired.

[0090] Fig. 15 is a process flow diagram illustrating example steps that may be implemented by an exemplary connection manager tracker. As part of a connection manager tracker process, a mobile device 10 may store a parameter table in memory or in a buffer which contains the values for a number of parameters related to the activity of various connection managers. These parameters may include a value for the current connection manager in use (CM in use), the last software build implemented on the mobile device (Last build used), and the software build implemented for the currently selected connection manager (Build for current CM). A mobile device 10 may be initialized by the OEM with certain values for each of these parameters. For example, the mobile device 10 may be initialized to set “CM in use,” “Last build used,” and “Build for current CM” parameters to “none.” At any time a processor 191 may receive a request to launch a connection manager supporting a particular service provider account, step 220. Upon receipt of the request to launch a connection manager, the processor 191 may determine if a connection manager is currently running, decision 225. The processor 191 may make this determination by checking the value stored in the parameter table stored in memory for the “CM in use” value. If the “CM in use” value is anything other than “none”, then the processor 191 will determine that a connection manager is currently in use (i.e., decision 225 = Yes). If a connection manager is in use, then the processor 191 may display an error message to the user indicating that a connection manager is already running, step 230. The error message may optionally indicate that if the user desires to switch connection managers then the currently active connection manager should be closed before launching the currently selected connection manager. Once the error message is displayed to the user, the processor 191 may await the next connection manager launch request or selection of a different service provider, step 155.

[0091] If, however, the processor 191 determines that no connection manager is currently running, the processor 191 enters a value for the “CM in use” parameter as the name of the service provider of the selected connection

manager request, step 235. The processor 191 also changes the value of the “Build for current CM” parameter in the parameter table to the name of the service provider of the selected connection manager request, step 240. The processor 191 may determine if the connection manager currently selected for launch is the same as or different from the last connection manager launched, decision 245. The processor 191 may compare the values of the parameters of the “Build for current CM” and “Last Build Used” stored in the parameter table. In instances where the mobile device 10 is being used for the first time to enable communication capabilities, the value of the parameter “Last Build Used” will be the initialized value of “none.” As a result, the comparison of the “Build for current CM” parameter value will not match the value of the “Last Build Used” parameter (i.e., decision 245 = No). In addition, if the user has selected to launch a connection manager different from the connection manager launched immediately prior to the instant connection manager, the comparison of the “Build for Current CM” and “Last Build Used” parameter will not result in a match (i.e., decision 245 = No). If the comparison of the “Build for Current CM” and “Last Build Used” parameters does not result in a match (i.e., decision 245 = No), the processor may implement the process flow to re-program the mobile device 10 described above with reference to Fig. 6, step 250. Once the mobile device 10 has been reprogrammed with the software build for the selected service provider account, the processor 191 may set the value of the “Last Build Used” parameter to indicate that the last build used is the software build of the currently selected service provider, step, 255. Once the new value of the “Last Build Used” parameter is stored in memory, the processor 191 may await the next connection manager launch request or selection of a different service provider, step 155.

[0092] If the comparison of the “Build for Current CM” and “Last Build Used” parameters results in a match (i.e., decision 245 = Yes), then the processor 191 does not have to re-program the mobile device 10 with a new software build and the previously loaded software build may continue to support

communications. Consequently, the processor 191 may set the value of the “Last Build Used” parameter to indicate that the last build used is the software build of the currently selected service provider, step, 255. Once the new value of the “Last Build Used” parameter is stored in memory, the processor 191 may await the next connection manager launch request or selection of a different service provider, step 155. In an optional embodiment, the processor 191 may simply skip step 255 and await the next connection manager launch request, step or selection of a different service provider.

[0093] When a user elects to disable the communication capabilities of the mobile device 10, the user may close any currently running connection manager. In such instances, the processor 191 will close the currently running connection manager and set the value of “CM in Use” parameter to “none.”

[0094] The embodiments described above may also be implemented on any of a variety of server systems such as illustrated in Fig. 16. Such a server 309 typically includes a processor 361 coupled to volatile memory 362 and a large capacity nonvolatile memory, such as a disk drive 363. The processor 361 is coupled to one or more network interface circuits, such as high speed modems 364 coupled to a network 365 such as the Internet. The computer 360 may also include a portable media reader, such as a compact disc (CD) drive 366 coupled to the processor 361.

[0095] Those of skill in the art would appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may

implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[0096] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in processor readable memory which may be any of RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to a processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal or mobile device. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal or mobile device. Additionally, in some aspects, the steps and/or actions of a method or algorithm may reside as one or any combination or set of codes and/or instructions on a machine readable medium and/or computer readable medium, which may be incorporated into a computer program product.

[0097] The foregoing description of the various embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein, and instead the claims should be accorded the widest scope consistent with the principles and novel features disclosed herein.

CLAIMS

What is claimed is:

1. A method of preventing simultaneous connection manager activation on a mobile device comprising:

receiving a request to launch a first connection manager supporting a first service provider account;

determining whether a second connection manager supporting a second service provider account is already active; and

preventing a first connection manager from launching until the second connection manager is closed if the second connection manager is already active.

2. The method of claim 1, further comprising:

initializing a parameters value indicating a status of a current connection manager in use, parameter value indicating a status of a software build for the current connection manager, and a parameter value indicating a status of a last software build used; and

storing the initialized parameter values in a memory,

wherein determining whether the second connection manager supporting the second service provider account is already active comprises determining if the current connection manager parameter value has been changed from its initialized value.

3. The method of claim 1, further comprising displaying an error message indicating that the first connection manager may not be launched if the parameter value of current connection manager has been changed from its initialized value.

4. The method of claim 3, wherein the error message indicates that the second connection manager must be closed before launching the first connection manager.

5. The method of claim 2, further comprises:

changing the current connection manager parameter value and software build for the current connection manager parameter value stored in memory to indicate a service provider supporting the first connection manager;

comparing the software build for current connection manager parameter value to the last software build used parameter value;

programming and provisioning the mobile device with a software build for the service provider supporting the first connection manager if the software build for current connection manager parameter value does not match the last software build used parameter value; and

changing the last software build used parameter value stored in memory to indicate the service provider supporting the first connection manager.

6. The method of claim 1, further comprising:

receiving a request to close the second connection manager; and

re-initializing the parameters values indicating a status of connection manager in use parameters value, the software build for current connection manager parameters value, and last software build used parameters values.

7. A mobile device comprising:

means for receiving a request to launch a first connection manager supporting a first service provider account;

means for determining whether a second connection manager supporting a second service provider account is already active; and

means for preventing a first connection manager from launching until the second connection manager is closed if the second connection manager is already active.

8. The mobile device of claim 7, further comprising:

means for initializing a parameters value indicating a status of a current connection manager in use, parameter value indicating a status of a software build for the current connection manager, and a parameter value indicating a status of a last software build used; and

means for storing the initialized parameter values in a memory,

wherein means for determining whether the second connection manager supporting the second service provider account is already active comprises means for determining if the current connection manager parameter value has been changed from its initialized value.

9. The mobile device of claim 7, further comprising means for displaying an error message indicating that the first connection manager may not be launched if the parameter value of current connection manager has been changed from its initialized value.

10. The mobile device of claim 9, wherein the means for displaying an error message indicates that the second connection manager must be closed before launching the first connection manager.

11. The mobile device of claim 8, further comprises:

means for changing the current connection manager parameter value and software build for the current connection manager parameter value stored in memory to indicate a service provider supporting the first connection manager;

means for comparing the software build for current connection manager parameter value to the last software build used parameter value;

means for programming and provisioning the mobile device with a software build for the service provider supporting the first connection manager if the software build for current connection manager parameter value does not match the last software build used parameter value; and

means for changing the last software build used parameter value stored in memory to indicate the service provider supporting the first connection manager.

12. The mobile device of claim 7, further comprising:

means for receiving a request to close the second connection manager;
and

means for re-initializing the parameters values indicating a status of connection manager in use parameters value, the software build for current connection manager parameters value, and last software build used parameters values.

13. A mobile device, comprising:

an internal memory unit, the internal memory unit including a provisioning data buffer; and

a processor coupled to the internal memory unit, wherein the processor is configured with software instructions to perform steps comprising:

receiving a request to launch a first connection manager supporting a first service provider account;

determining whether a second connection manager supporting a second service provider account is already active; and

preventing a first connection manager from launching until the second connection manager is closed if the second connection manager is already active.

14. The mobile device of claim 13, wherein the processor is configured with software instructions to perform further steps comprising:

initializing a parameters value indicating a status of a current connection manager in use, parameter value indicating a status of a software build for the current connection manager, and a parameter value indicating a status of a last software build used; and

storing the initialized parameter values in a memory,

wherein determining whether the second connection manager supporting the second service provider account is already active comprises determining if the current connection manager parameter value has been changed from its initialized value.

15. The mobile device of claim 13, wherein the processor is configured with software instructions to perform further steps comprising displaying an error message indicating that the first connection manager may not be launched if the parameter value of current connection manager has been changed from its initialized value.

16. The mobile device of claim 15, wherein the error message indicates that the second connection manager must be closed before launching the first connection manager.

17. The mobile device of claim 14, wherein the processor is configured with software instructions to perform further steps comprising:

changing the current connection manager parameter value and software build for the current connection manager parameter value stored in memory to indicate a service provider supporting the first connection manager;

comparing the software build for current connection manager parameter value to the last software build used parameter value;

programming and provisioning the mobile device with a software build for the service provider supporting the first connection manager if the software build for current connection manager parameter value does not match the last software build used parameter value; and

changing the last software build used parameter value stored in memory to indicate the service provider supporting the first connection manager.

18. The mobile device of claim 13, wherein the processor is configured with software instructions to perform further steps comprising:

- receiving a request to close the second connection manager; and
- re-initializing the parameters values indicating a status of connection manager in use parameters value, the software build for current connection manager parameters value, and last software build used parameters values.

19. A tangible storage medium having stored thereon processor-executable software instructions configured to cause a processor to perform steps comprising:

- receiving a request to launch a first connection manager supporting a first service provider account;
- determining whether a second connection manager supporting a second service provider account is already active; and
- preventing a first connection manager from launching until the second connection manager is closed if the second connection manager is already active.

20. The tangible storage medium of claim 19, wherein the tangible storage medium has processor-executable software instructions configured to cause a processor to perform further steps comprising:

- initializing a parameters value indicating a status of a current connection manager in use, parameter value indicating a status of a software build for the current connection manager, and a parameter value indicating a stats of a last software build used; and

- storing the initialized parameter values in a memory,
- wherein determining whether the second connection manager supporting the second service provider account is already active comprises determining if the current connection manager parameter value has been changed from its initialized value.

21. The tangible storage medium of claim 19, wherein the tangible storage medium has processor-executable software instructions configured to cause a processor to perform further steps comprising:

displaying an error message indicating that the first connection manager may not be launched if the parameter value of current connection manager has been changed from its initialized value.

22. The tangible storage medium of claim 21, wherein the error message indicates that the second connection manager must be closed before launching the first connection manager.

23. The tangible storage medium of claim 20, wherein the tangible storage medium has processor-executable software instructions configured to cause a processor to perform further steps comprising:

changing the current connection manager parameter value and software build for the current connection manager parameter value stored in memory to indicate a service provider supporting the first connection manager;

comparing the software build for current connection manager parameter value to the last software build used parameter value;

programming and provisioning the mobile device with a software build for the service provider supporting the first connection manager if the software build for current connection manager parameter value does not match the last software build used parameter value; and

changing the last software build used parameter value stored in memory to indicate the service provider supporting the first connection manager.

24. The tangible storage medium of claim 19, wherein the tangible storage medium has processor-executable software instructions configured to cause a processor to perform further steps comprising:

receiving a request to close the second connection manager; and

re-initializing the parameters values indicating a status of connection manager in use parameters value, the software build for current connection manager parameters value, and last software build used parameters values.

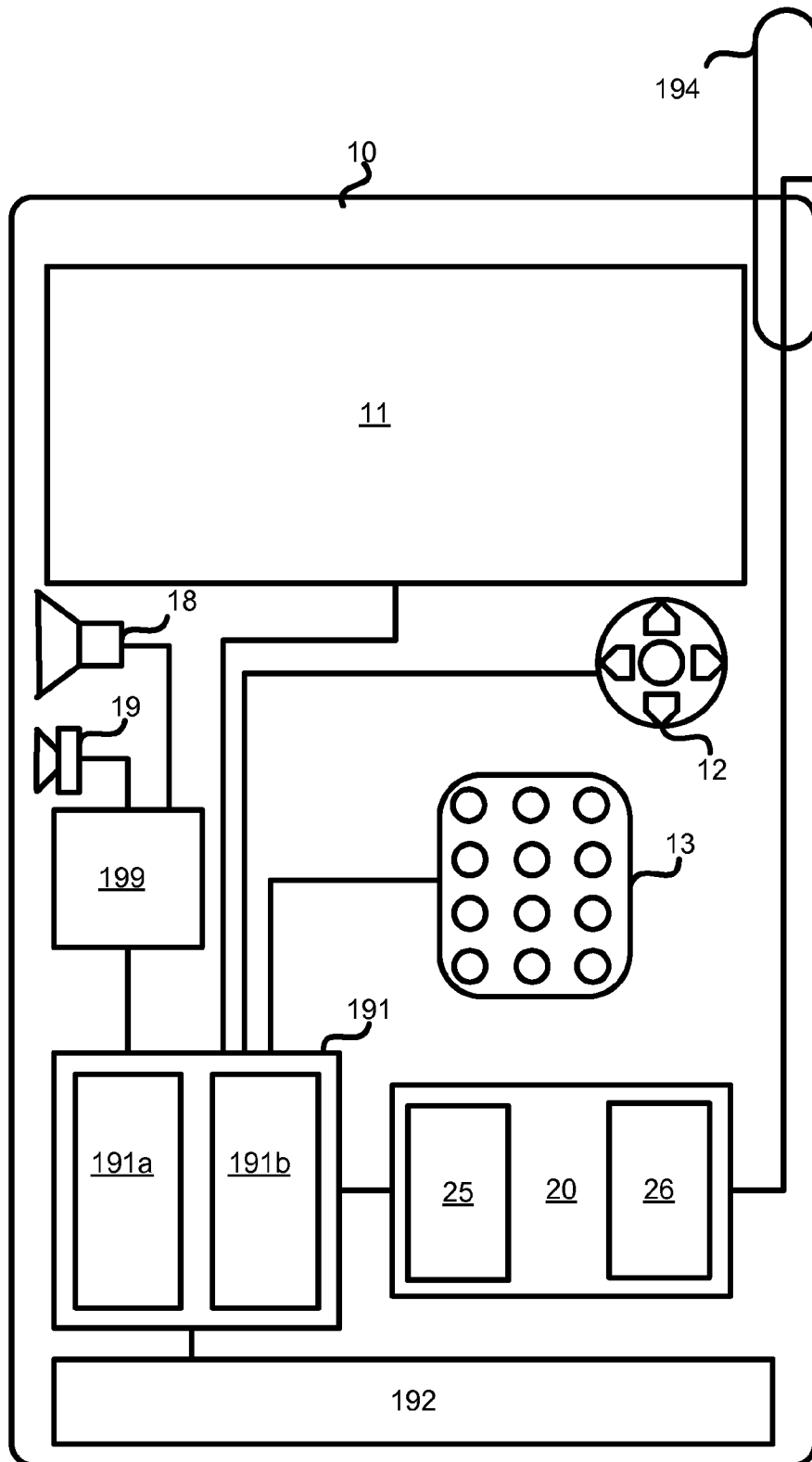


Fig. 1

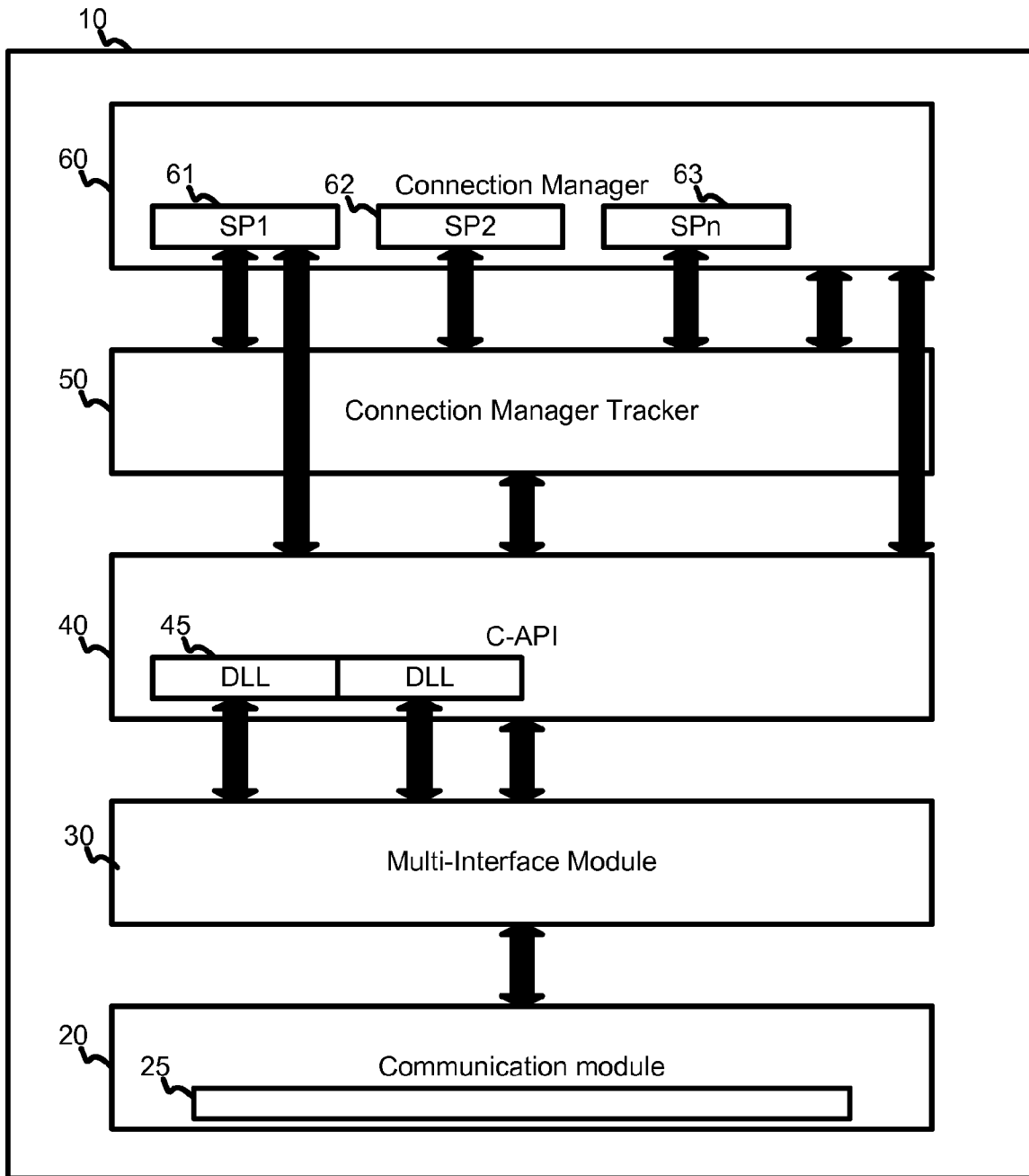


Fig. 2

Parameter/Setting	Service Provider 1	Service Provider 2	Service Provider 3	Service Provider 4
Mode of Activation	OTASP	IOTA	OTASP	IOTA
NAI MIP User Profile N, where N = {0, 1, 2, ...}	MDN@SP1.com	MEID@nem.SP2.com	MDN@1x.SCP3mobility.com	0000WXYZ@ota.1x.SF4.cs
NAI MIP User Profile N, where N = {0, 1, 2, ...}	Not used	name@SP2.com	Not Used	MDN@3g.1x.SF4.cs
MN-HA Shared Secret MIP User Profile N, where N = {0, 1, 2, ...}	All zeros (16 Bytes) after DMU update it gets changed	"secret"	First 16 digits of Akey	8 character pESN is Upper Case
MN-HA Shared Secret MIP User Profile N, where N = {0, 1, 2, ...}	Not used	"secret"	Not Used	8 character pESN is Upper Case
MN-AAA Shared Secret MIP User Profile N, where N = {0, 1, 2, ...}	All zeros (16 Bytes)	MD5 (Akey/MEID)	MEID	Factory Default Password = MD5(NAI), where NAI is the factory default NAI Hardcoded after MDN Programmed = MD5 Function0 (NAI, Iota), where NAI is the hardcoded NAI
MN-AAA Shared Secret MIP User Profile N, where N = {0, 1, 2, ...}	Not used	8 character (populated by IOTA)	Not Used	MD5 (Akey + "anasa" + MEID)
SIP AAA NAI	MDN@SP1.com	Not Used	MDN@1x.SP3.com	Not Used
SIP AAA Password	All zeros before DMU Update	Not Used	MEID HEX 14 Digit	Not Used

Fig. 3

Parameter/Setting	Service Provider 1	Service Provider 2	Service Provider 3	Service Provider 4
MN Authenticator	1111base10	Not required	Not required	Not required
MN HA SPI Set	Enable	Enable	Enable	Enable
MN HA SPI Value	300	1234	200 (512)	1235
MN AAA SPI Set	Enable	Enable	Enable	Enable
MN AAA SPI Value	2	1234	2	2
Reverse Tunneling	Enable	Enable	Enable	Enable
QNC Enabled	Enable	Disable	Disable	Disable
Home Address	0.0.0.0	0.0.0.0	000.000.000.000	Not Used
Primary HA Address (0, 1)	Dynamic, no Slot 1 Usage 255.255.255.255	IOTA HA Address needs to be written in Slot-0, Slot-1 HA Address is populated by IOTA, need to leave them as <null string>	255.255.255.255 (Single slot used for data)	IOTA HA Address needs to be written in Slot-0, Slot-1 HA Address is populated by IOTA, need to leave them as <null string>
Secondary HA Address(0, 1)	255.255.255.255	IOTA HA Address needs to be written in Slot-0, Slot-1 HA Address is populated by IOTA, need to leave them as <null string>	0.0.0.0	IOTA HA Address needs to be written in Slot-0, Slot-1 HA Address is populated by IOTA, need to leave them as <null string>
Initial Registrations Retry Interval Time	3	4	2	4
Registry Retry Number	2	1	2	1
DS MIP Deregistration Retries	2	1	2	
Pre-Lifetime-expiry RE- registration time	0	30	30	30

Fig. 4

Parameter/Setting	Service Provider 1	Service Provider 2	Service Provider 3	Service Provider 4
SPC	"000000"	8 digit random number (Should match with EDF info)	8 digit random number	8 digit random number
OTKSL	"000000"	8 digit random number (Should match with EDF info)	8 digit random number (also requires CSL)	8 digit random number
Number of Incorrect SPC Attempts	15	5	?	5
Field Service Code	"000000" (vendor proprietary)	"040793"	vendor proprietary	vendor proprietary
Akey Checksum	Generic	Vendor proprietary (Should match EDF info)	Generic	Generic
SMS Support	Yes	No	Yes	Yes (Need to Confirm)

Fig. 5

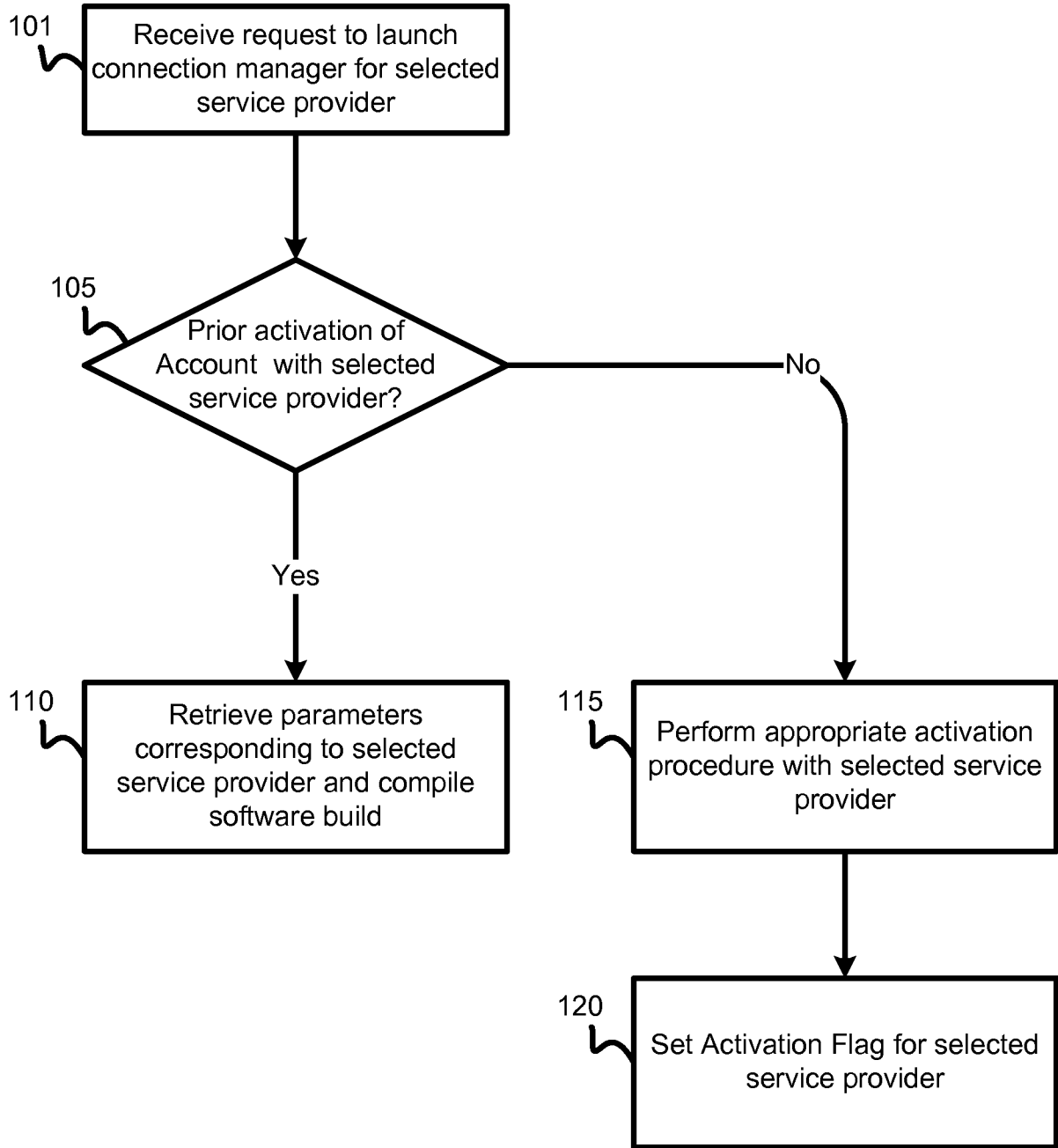


Fig. 6

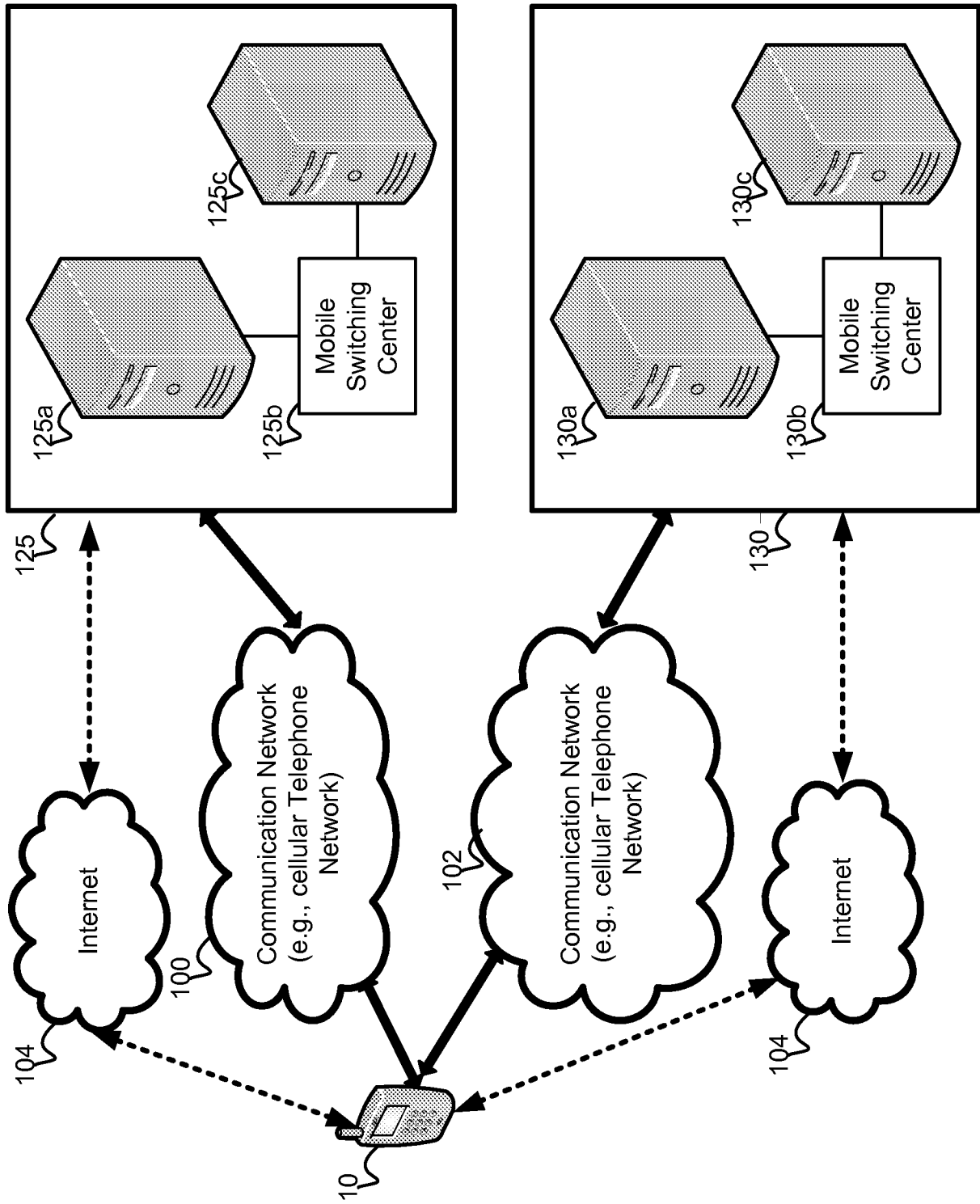


Fig. 7

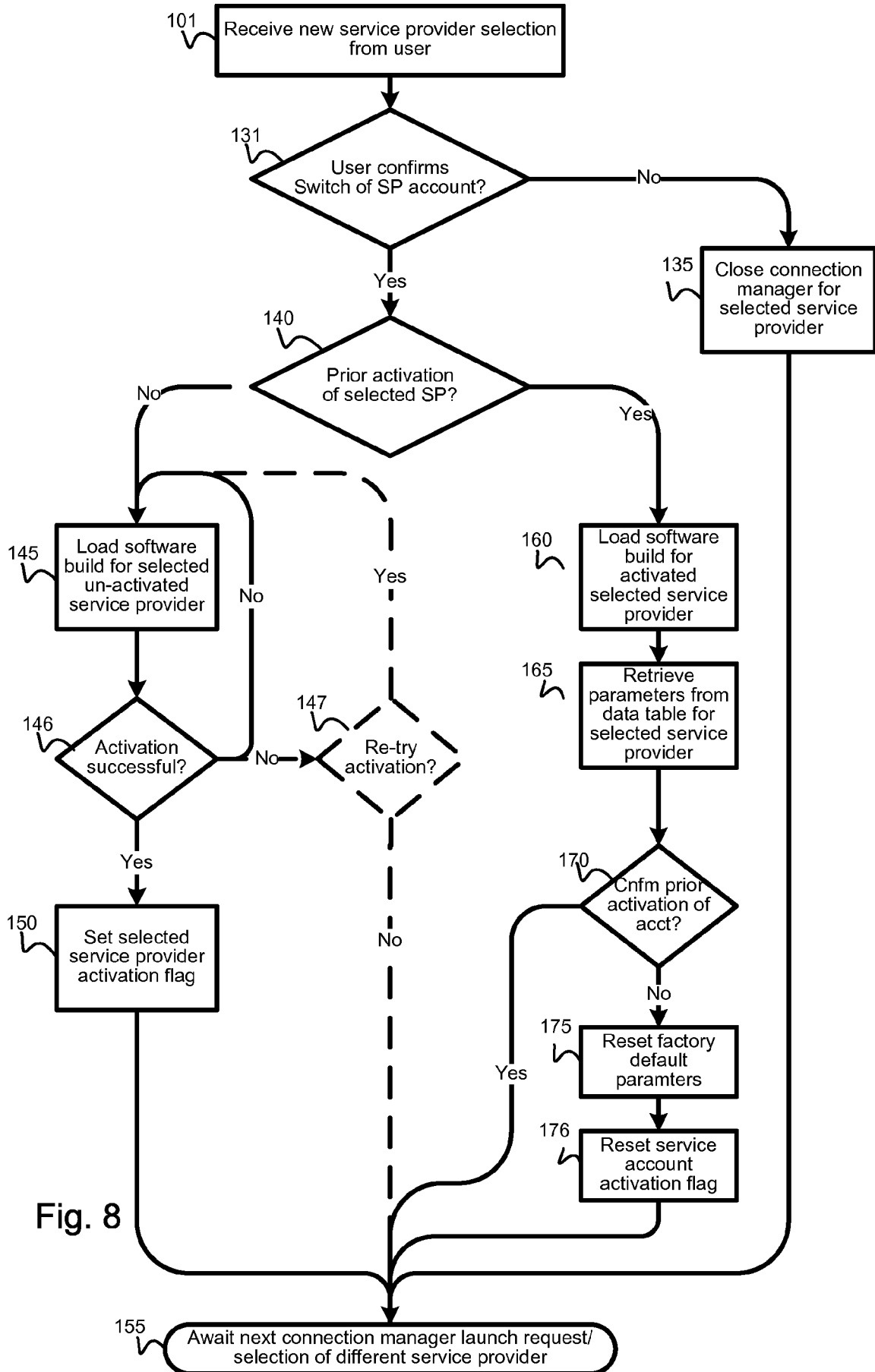


Fig. 8

9/16

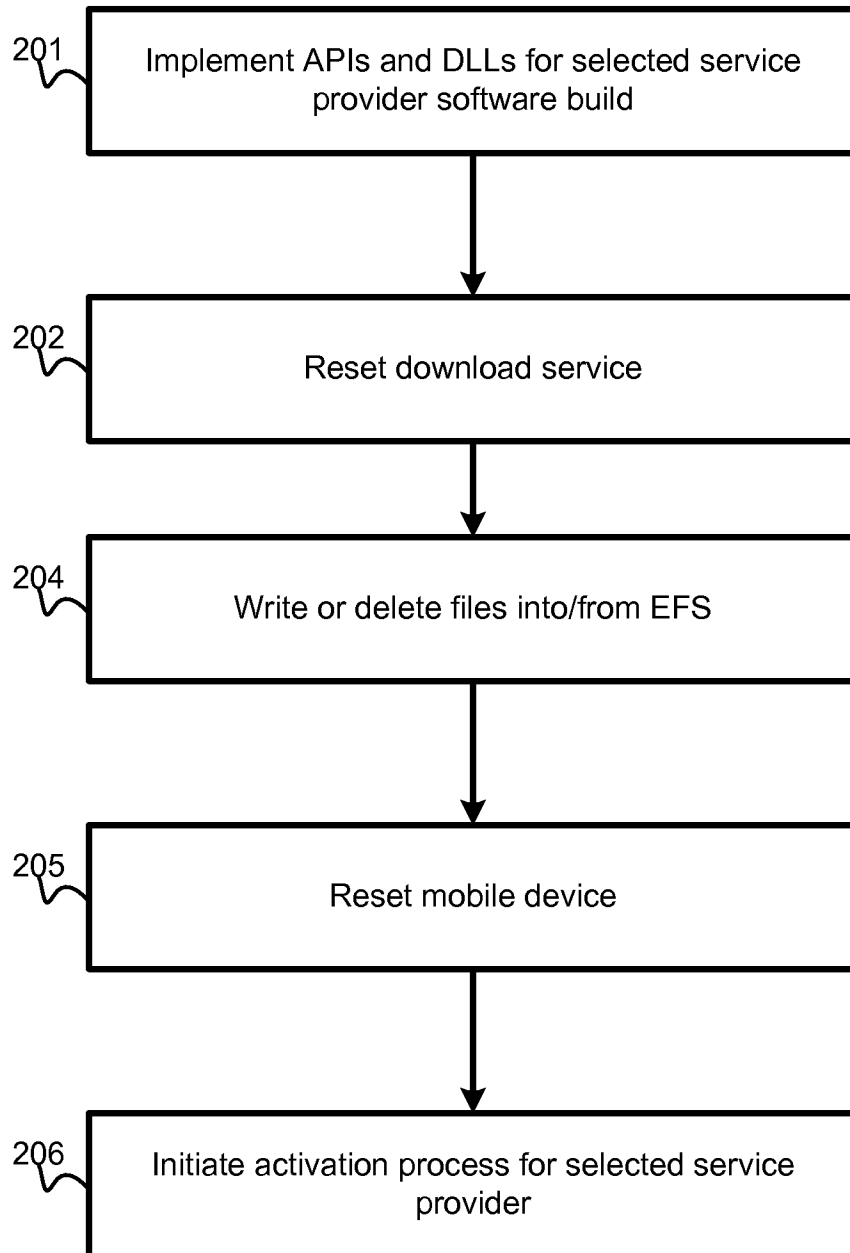


Fig. 9

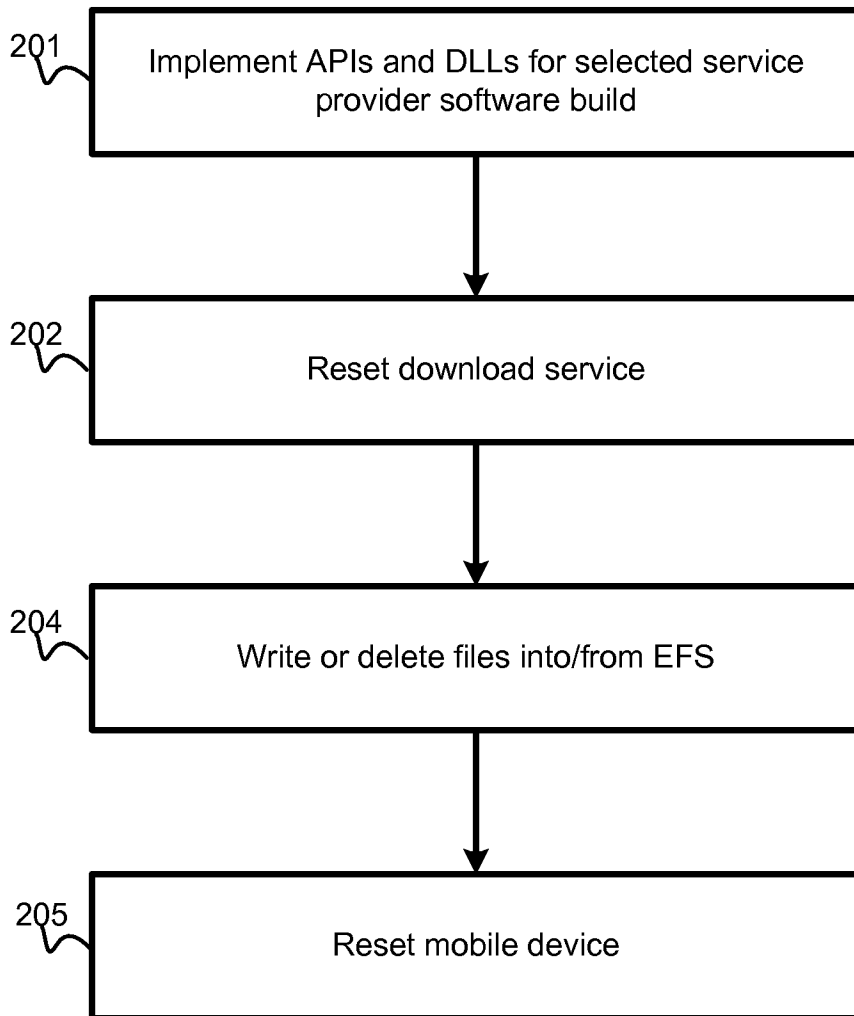


Fig. 10

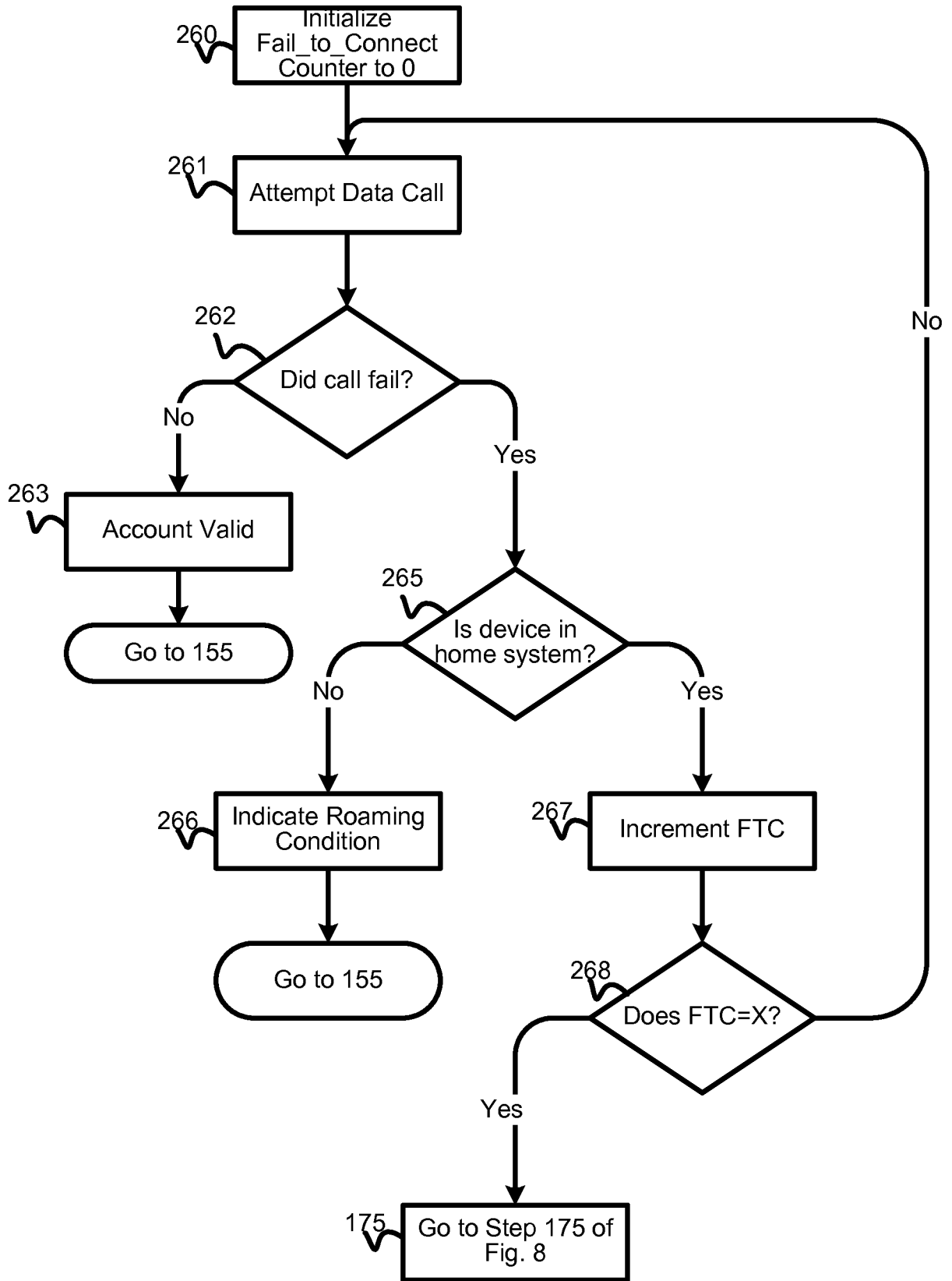


Fig. 11

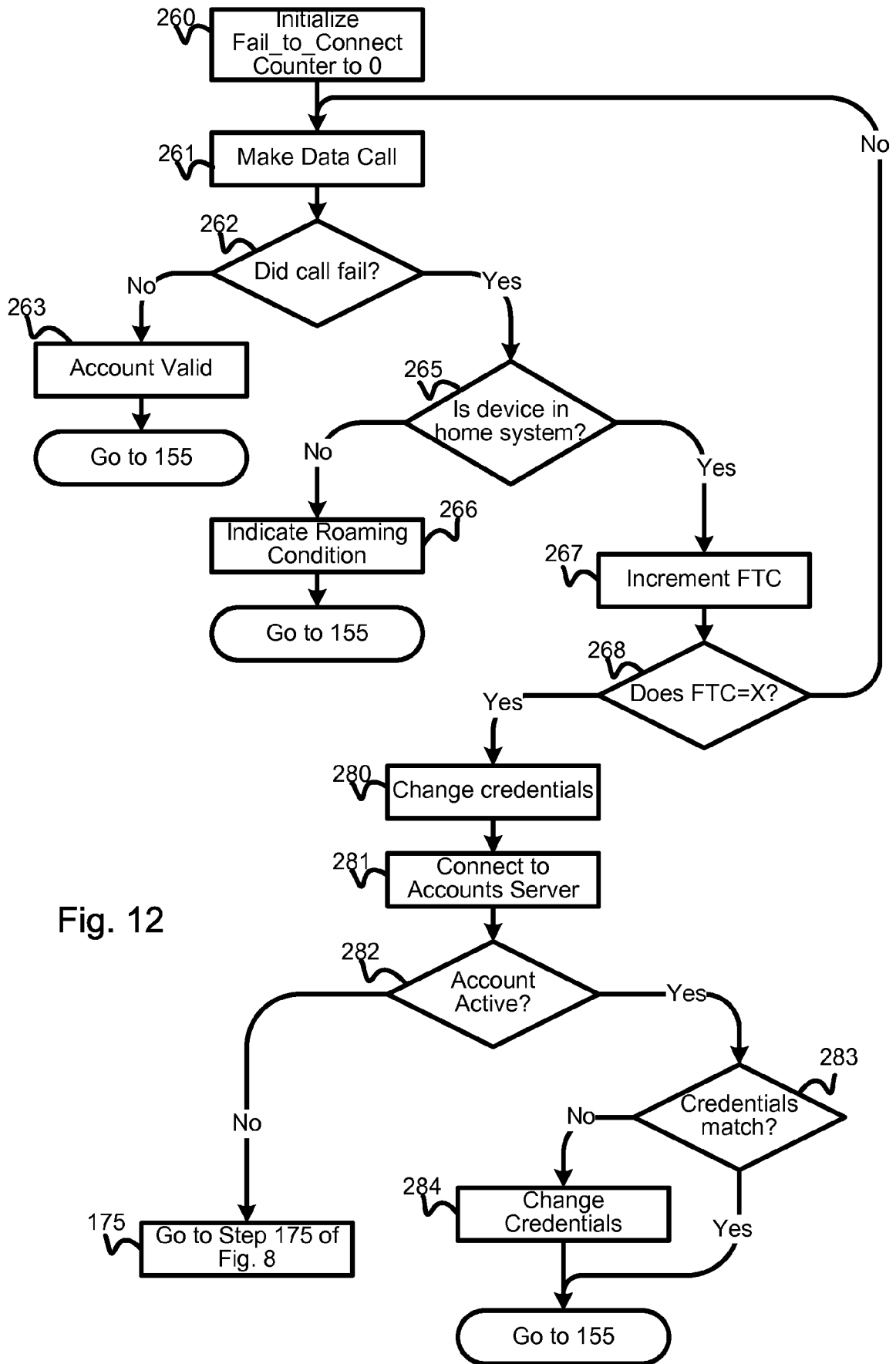


Fig. 12

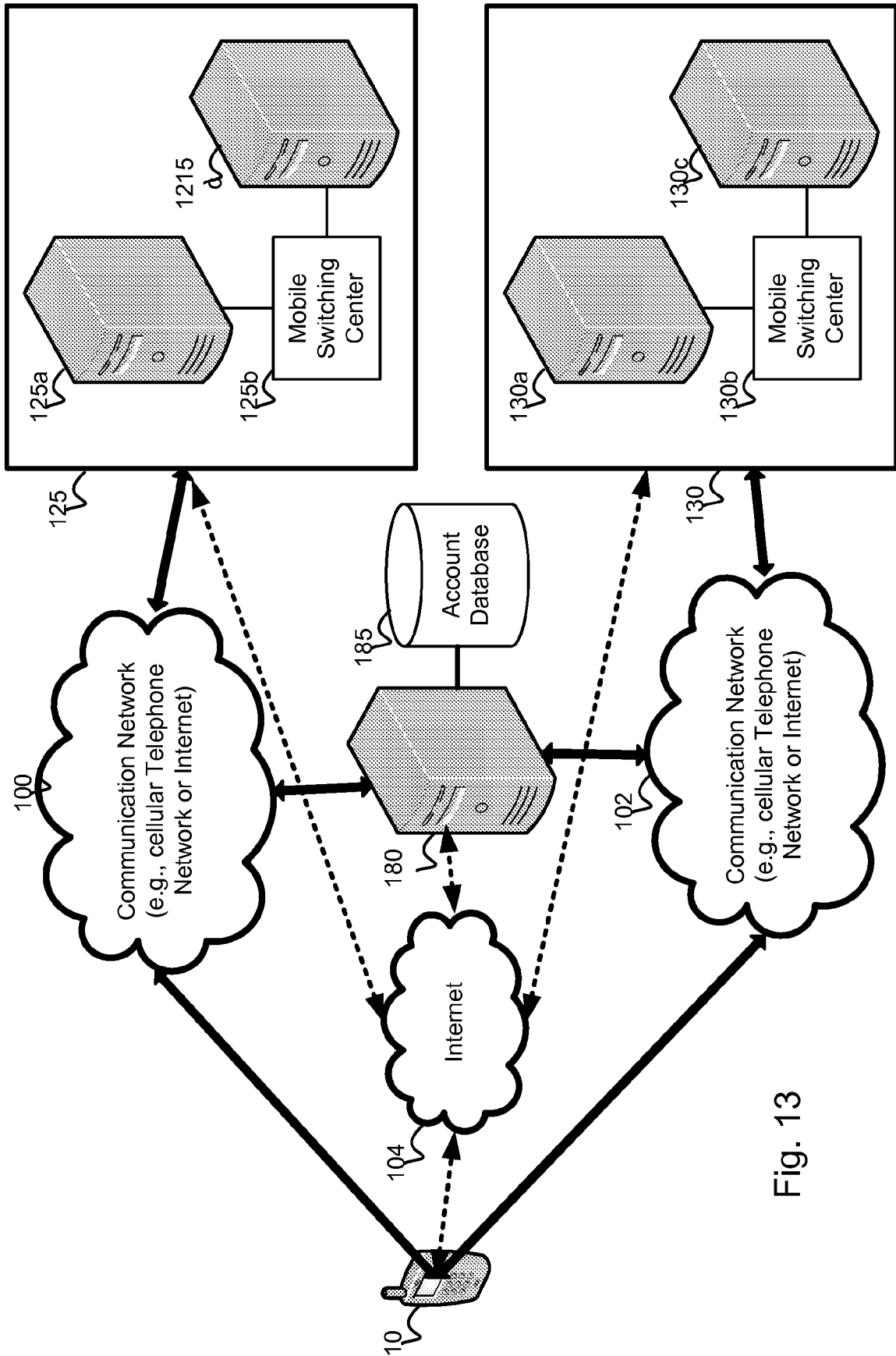


Fig. 13

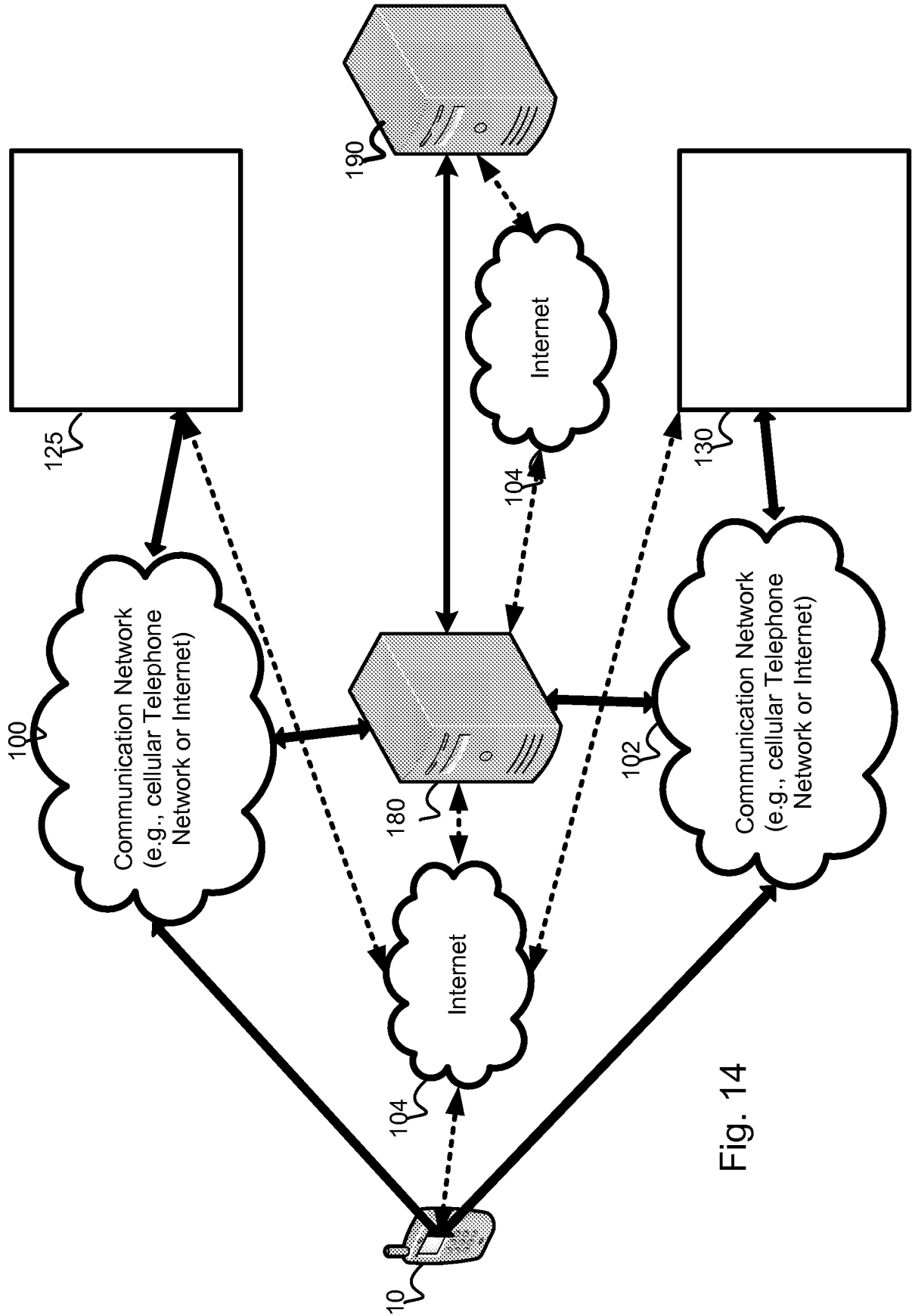


Fig. 14

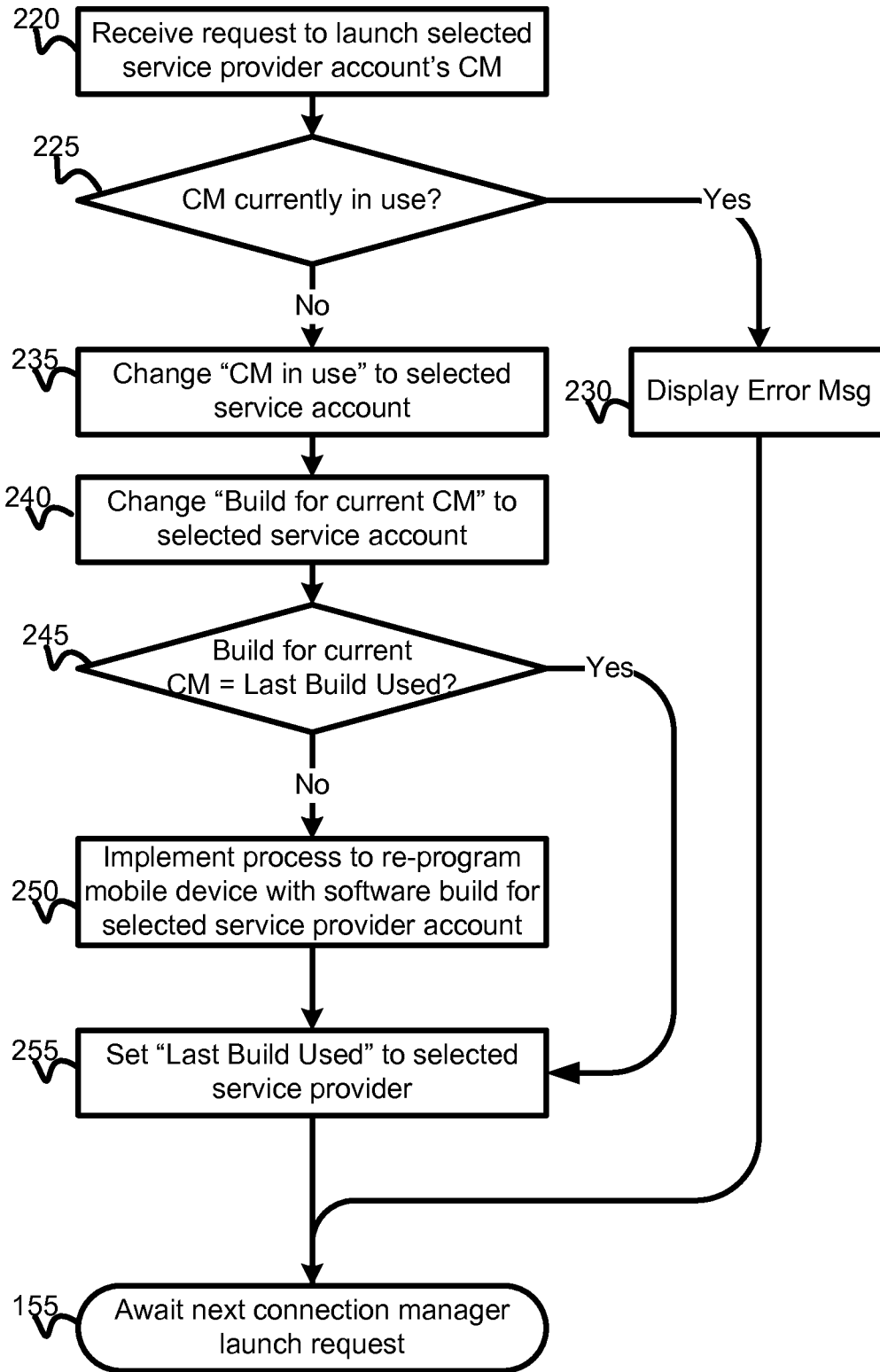


Fig. 15

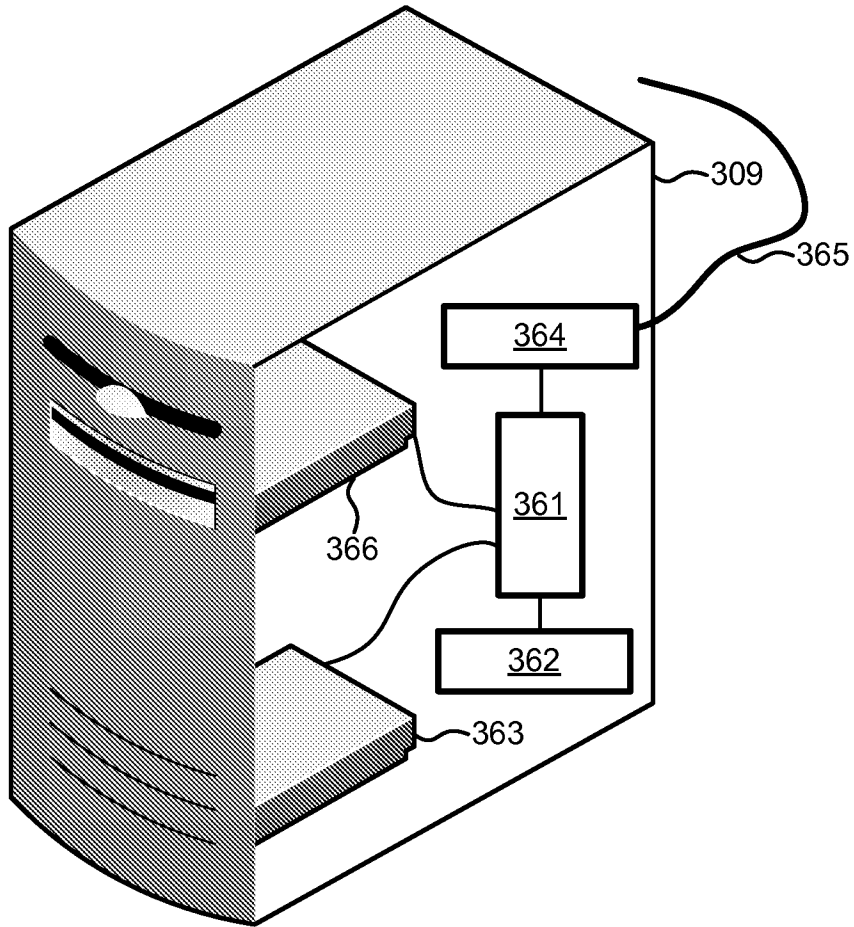


Fig. 16

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2010/035145

A. CLASSIFICATION OF SUBJECT MATTER INV. H04W8/18 ADD.		
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) H04W		
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		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/018853 A1 (LEWIS JONATHAN D [GB]) 29 January 2004 (2004-01-29)	1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 18, 19, 21, 22, 24
A	paragraph [0045] paragraph [0049] paragraph [0055] - paragraph [0056]	2, 5, 8, 11, 14, 17, 20, 23
A	EP 1 473 845 A1 (SONY ERICSSON MOBILE COMM AB [SE]) 3 November 2004 (2004-11-03) paragraph [0016]	1-24
<input type="checkbox"/> Further documents are listed in the continuation of Box C.		
<input checked="" type="checkbox"/> 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 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. *Z* document member of the same patent family	
Date of the actual completion of the international search <p style="text-align: center; font-weight: bold;">19 October 2010</p>	Date of mailing of the international search report <p style="text-align: center; font-weight: bold;">26/10/2010</p>	
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer <p style="text-align: center; font-weight: bold;">Marín Saldaña, I</p>	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2010/035145

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
US 2004018853	A1	29-01-2004	CN 1509521 A	30-06-2004
			GB 2386504 A	17-09-2003
			GB 2406482 A	30-03-2005
			WO 03077437 A2	18-09-2003
			JP 2005519562 T	30-06-2005
EP 1473845	A1	03-11-2004	WO 2004098081 A1	11-11-2004