terminal 1000 and/or one or more mobile companions. The display 1004 provides for graphics based alphanumerical information such as, for example, the price of an item requested by the user. The display 1004 also provides for the display of graphics such as icons representative of particular menu items, for example. The display 1004 can also be a touch screen, which can employ capacitive, resistive touch, infrared, surface acoustic wave, or grounded acoustic wave technology.

[0073] The handheld terminal 1000 further includes user input keys 1006 for allowing a user to input information and/or operational commands. The user input keys 1006 can include a full alphanumeric keypad, function keys, enter keys, *etc.* The handheld terminal 1000 can also include a magnetic strip reader 1008 or other data capture mechanism (not shown). An electronic signature apparatus can also be employed in connection with the magnetic strip reader or a telecheck system.

[0074] The handheld terminal 1000 can also include a window 1010 in which a bar code reader/bar coding imager is able to read a bar code label, or the like, presented to the handheld terminal 1000. The handheld terminal 1000 can include a light emitting diode (LED) (not shown) that is illuminated to reflect whether the bar code has been properly or improperly read. Alternatively, or additionally, a sound can be emitted from a speaker (not shown) to alert the user that the bar code has been successfully imaged and decoded. The handheld terminal 1000 also includes an antenna (not shown) for wireless communication with a radio frequency (RF) access point; and an infrared (IR) transceiver (not shown) for communication with an IR access point.

[0075] FIG. 11 is a schematic block diagram of a sample-computing environment 1100 with which the invention can interact. The system 1100 includes one or more client(s) 1110. The client(s) 1110 can be hardware and/or software (*e.g.*, threads, processes, computing devices). The system 1100 also includes one or more server(s) 1120. The server(s) 1120 can also be hardware and/or software (*e.g.*, threads, processes, computing devices). The servers 1120 can house threads to perform transformations by employing the invention, for example.

[0076] One possible communication between a client 1110 and a server 1120 can be in the form of a data packet adapted to be transmitted between two or more computer processes. The system 1100 includes a communication framework 1140 that can be employed to facilitate communications between the client(s) 1110 and the server(s) 1120. The client(s) 1110 are operably connected to one or more client data

store(s) 1150 that can be employed to store information local to the client(s) 1110. Similarly, the server(s) 1120 are operably connected to one or more server data store(s) 1130 that can be employed to store information local to the servers 1140.

[0077] With reference to FIG. 12, an exemplary environment 1210 for implementing various aspects of the invention includes a computer 1212. The computer 1212 includes a processing unit 1214, a system memory 1216, and a system bus 1218. The system bus 1218 couples system components including, but not limited to, the system memory 1216 to the processing unit 1214. The processing unit 1214 can be any of various available processors. Dual microprocessors and other multiprocessor architectures also can be employed as the processing unit 1214.

[0078] The system bus 1218 can be any of several types of bus structure(s) including the memory bus or memory controller, a peripheral bus or external bus, and/or a local bus using any variety of available bus architectures including, but not limited to, Industrial Standard Architecture (ISA), Micro-Channel Architecture (MSA), Extended ISA (EISA), Intelligent Drive Electronics (IDE), VESA Local Bus (VLB), Peripheral Component Interconnect (PCI), Card Bus, Universal Serial Bus (USB), Advanced Graphics Port (AGP), Personal Computer Memory Card International Association bus (PCMCIA), Firewire (IEEE 1394), and Small Computer Systems Interface (SCSI).

[0079] The system memory 1216 includes volatile memory 1220 and nonvolatile memory 1222. The basic input/output system (BIOS), containing the basic routines to transfer information between elements within the computer 1212, such as during start-up, is stored in nonvolatile memory 1222. By way of illustration, and not limitation, nonvolatile memory 1222 can include read only memory (ROM), programmable ROM (PROM), electrically programmable ROM (EPROM), electrically erasable ROM (EEPROM), or flash memory. Volatile memory 1220 includes random access memory (RAM), which acts as external cache memory. By way of illustration and not limitation, RAM is available in many forms such as synchronous RAM (SRAM), dynamic RAM (DRAM), synchronous DRAM (SDRAM), double data rate SDRAM (DDR SDRAM), enhanced SDRAM (ESDRAM), Synchlink DRAM (SLDRAM), and direct Rambus RAM (DRRAM).

[0080] Computer 1212 also includes removable/non-removable, volatile/non-volatile computer storage media. FIG. 12 illustrates, for example a disk storage 1224. Disk storage 1224 includes, but is not limited to, devices like a magnetic disk drive,

floppy disk drive, tape drive, Jaz drive, Zip drive, LS-100 drive, flash memory card, or memory stick. In addition, disk storage 1224 can include storage media separately or in combination with other storage media including, but not limited to, an optical disk drive such as a compact disk ROM device (CD-ROM), CD recordable drive (CD-R Drive), CD rewritable drive (CD-RW Drive) or a digital versatile disk ROM drive (DVD-ROM). To facilitate connection of the disk storage devices 1224 to the system bus 1218, a removable or non-removable interface is typically used such as interface 1226.

[0081] It is to be appreciated that FIG. 12 describes software that acts as an intermediary between users and the basic computer resources described in suitable operating environment 1210. Such software includes an operating system 1228. Operating system 1228, which can be stored on disk storage 1224, acts to control and allocate resources of the computer system 1212. System applications 1230 take advantage of the management of resources by operating system 1228 through program modules 1232 and program data 1234 stored either in system memory 1216 or on disk storage 1224. It is to be appreciated that the invention can be implemented with various operating systems or combinations of operating systems.

[0082] A user enters commands or information into the computer 1212 through input device(s) 1236. Input devices 1236 include, but are not limited to, a pointing device such as a mouse, trackball, stylus, touch pad, keyboard, microphone, joystick, game pad, satellite dish, scanner, TV tuner card, digital camera, digital video camera, web camera, and the like. These and other input devices connect to the processing unit 1214 through the system bus 1218 *via* interface port(s) 1238. Interface port(s) 1238 include, for example, a serial port, a parallel port, a game port, and a universal serial bus (USB). Output device(s) 1240 use some of the same type of ports as input device(s) 1236. Thus, for example, a USB port may be used to provide input to computer 1212, and to output information from computer 1212 to an output device 1240. Output adapter 1242 is provided to illustrate that there are some output devices 1240 like monitors, speakers, and printers, among other output devices 1240, which require special adapters. The output adapters 1242 include, by way of illustration and not limitation, video and sound cards that provide a means of connection between the output device 1240 and the system bus 1218. It should be noted that other devices and/or systems of devices provide both input and output capabilities such as remote computer(s) 1244.

[0083] Computer 1212 can operate in a networked environment using logical connections to one or more remote computers, such as remote computer(s) 1244. The remote computer(s) 1244 can be a personal computer, a server, a router, a network PC, a workstation, a microprocessor based appliance, a peer device or other common network node and the like, and typically includes many or all of the elements described relative to computer 1212. For purposes of brevity, only a memory storage device 1246 is illustrated with remote computer(s) 1244. Remote computer(s) 1244 is logically connected to computer 1212 through a network interface 1248 and then physically connected *via* communication connection 1250. Network interface 1248 encompasses communication networks such as local-area networks (LAN) and wide-area networks (WAN). LAN technologies include Fiber Distributed Data Interface (FDDI), Copper Distributed Data Interface (CDDI), Ethernet, Token Ring and the like. WAN technologies include, but are not limited to, point-to-point links, circuit switching networks like Integrated Services Digital Networks (ISDN) and variations thereon, packet switching networks, and Digital Subscriber Lines (DSL).

[0084] Communication connection(s) 1250 refers to the hardware/software employed to connect the network interface 1248 to the bus 1218. While communication connection 1250 is shown for illustrative clarity inside computer 1212, it can also be external to computer 1212. The hardware/software necessary for connection to the network interface 1248 includes, for exemplary purposes only, internal and external technologies such as, modems including regular telephone grade modems, cable modems and DSL modems, ISDN adapters, and Ethernet cards.

[0085] What has been described above includes examples of the invention. It is, of course, not possible to describe every conceivable combination of components or methodologies for purposes of describing the subject invention, but one of ordinary skill in the art may recognize that many further combinations and permutations of the invention are possible. Accordingly, the invention is intended to embrace all such alterations, modifications, and variations that fall within the spirit and scope of the appended claims.

[0086] In particular and in regard to the various functions performed by the above described components, devices, circuits, systems and the like, the terms (including a reference to a "means") used to describe such components are intended to correspond, unless otherwise indicated, to any component which performs the specified function of the described component (*e.g.*, a functional equivalent), even

though not structurally equivalent to the disclosed structure, which performs the function in the herein illustrated exemplary aspects of the invention. In this regard, it will also be recognized that the invention includes a system as well as a computer-readable medium having computer-executable instructions for performing the acts and/or events of the various methods of the invention.

[0087] In addition, while a particular feature of the invention may have been disclosed with respect to only one of several implementations, such feature may be combined with one or more other features of the other implementations as may be desired and advantageous for any given or particular application. Furthermore, to the extent that the terms "includes," and "including" and variants thereof are used in either the detailed description or the claims, these terms are intended to be inclusive in a manner similar to the term "comprising."

CLAIMS

What is claimed is:

1. A portable communication device comprising:

a data analysis component that monitors stimuli associated with a device; and

a mobility policy manager (MPM) component that provides balancing of network connectivity and power consumption based at least in part upon the monitored stimuli.

2. The portable communication device of claim 1, the data analysis component monitors at least one of network traffic, an internet protocol address, and a port number.

3. The portable communication device of claim 1, the MPM component comprising a policy module that determines a policy based at least in part on the monitored stimuli.

4. The portable communication device of claim 1, the MPM component comprising an alter module that alters at least one policy to provide an optimal device power consumption.

5. The portable communication device of claim 4, the MPM component further comprising a tolerance parameter module that ensures the policy remains within a predetermined power consumption range.

6. The portable communication device of claim 1, the MPM component comprising a hysteresis module that prevents excessive altering between multiple device states.

7. The portable communication device of claim 1, the MPM component comprising a persistence module that allows the device to remain in a non-optimal state during a communication.

8. The portable communication device of claim 7, the non-optimal state is maintained until completion of the communication.

9. The portable communication device of claim 1, the MPM component comprising a packet route management module that controls a connectivity of a first network adapter and at least a second network adapter that are powered at a substantially similar time.

10. The portable communication device of claim 1, the MPM component comprising a designate module that designates at least one connection.

11. The portable communication device of claim 11, the designate module overrides a connection to force one of an outcome and a route.

12. The portable communication device of claim 1, the MPM component comprising a route module that hinders traffic in the absence of an appropriate route.

13. The portable communication device of claim 12, the route module comprising a categorization module that categorizes connections that distinguishes between requirements to create a new route and preference of an existing route.

14. The portable communication device of claim 12, the route module comprising a firewall module that restricts traffic if an appropriate route is not available.

15. A communication architecture, comprising:
a network that includes a plurality of resources;
a data analysis component that captures data about the plurality of resources; and a mobility policy manager (MPM) component that determines a policy to obtain efficient network connectivity and power consumption based at least in part on the captured data.

16. The communication architecture of claim 15, the captured data comprising at least one statistic based on network traffic associated with an Internet Protocol address or a port number end point.

17. The communication architecture of claim 15, the MPM component dynamically alters a predefined policy based at least in part upon the captured data.

18. A method for dynamically managing network connection performance, comprising:

creating an initial policy;

monitoring the initial policy; and

automatically altering the initial policy to achieve at least one policy objective.

19. The method of claim 18, the initial policy is created based upon at least one statistic derived from device conditions.

20. The method of claim 18, automatically altering the initial policy further comprising:

determining a state of a connection;

ascertaining if the connection is complete; and

maintaining the connection state until communication is complete.

21. The method of claim 18, automatically altering the initial policy further includes one of allowing, denying, and rejecting traffic.

22. A computer readable medium of a portable device to efficiently manage network connections, comprising:

a data analysis component operable to monitor device conditions; and

a mobility policy manager component that dynamically alters a policy to achieve at least one policy objective.

23. The computer readable medium of claim 22, the mobility policy manager provides balancing of network connectivity and power consumption based at least in part on the monitored device conditions.

24. The computer readable medium of claim 22, an initial policy is created based at least in part on the monitored device conditions.

25. A portable communication system, comprising:

means for monitoring device connectivity and power consumption;

means for creating a policy based at least in part on the monitored device connectivity and power consumption; and

means for altering the policy based on monitored operating conditions.

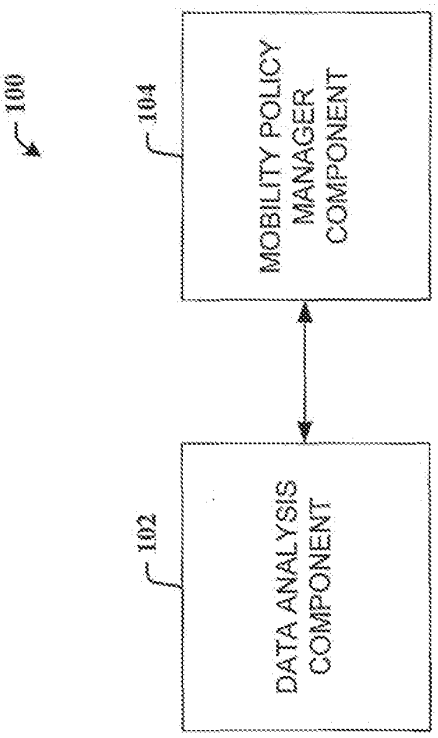

100
104
MOBILITY POLICY MANAGER COMPONENT
102
DATA ANALYSIS COMPONENT

FIG. 1

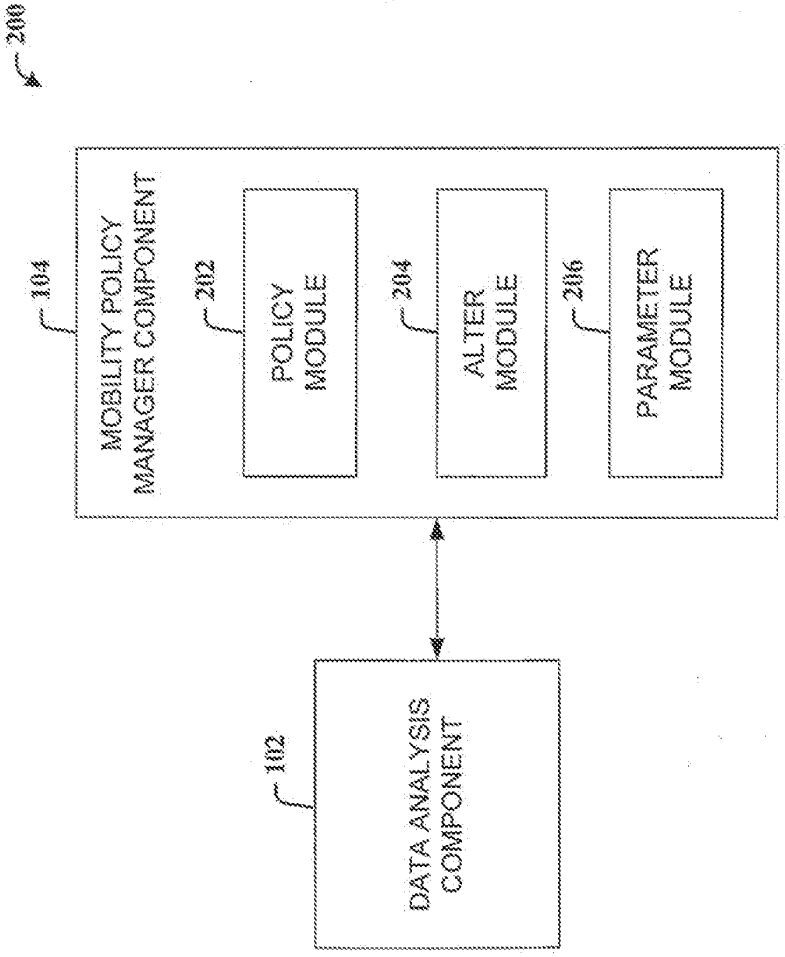

200
104
MOBILITY POLICY MANAGER COMPONENT
202
POLICY MODULE
204
ALTER MODULE
206
PARAMETER MODULE
102
DATA ANALYSIS COMPONENT

FIG. 2

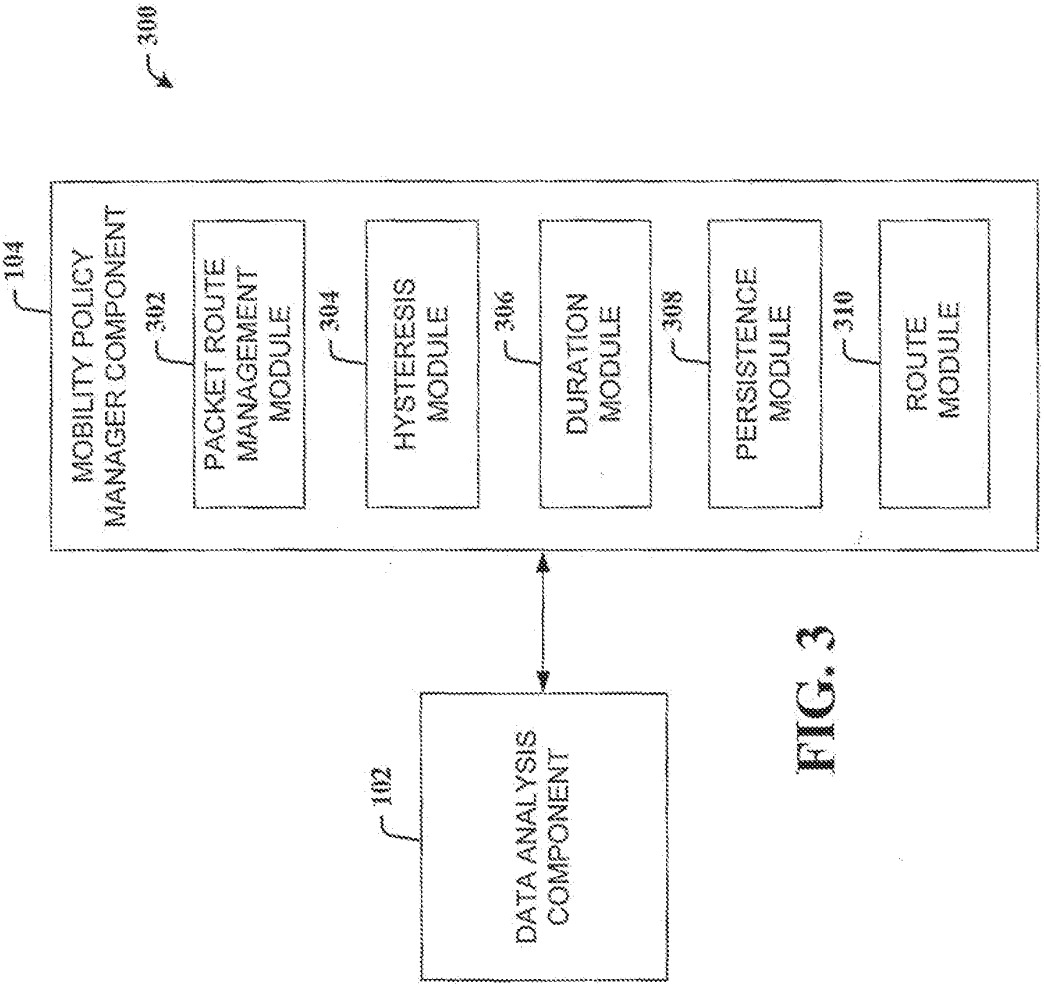

300
104
MOBILITY POLICY MANAGER COMPONENT
302
PACKET ROUTE MANAGEMENT MODULE
304
HYSTERESIS MODULE
306
DURATION MODULE
308
PERSISTENCE MODULE
310
ROUTE MODULE
102
DATA ANALYSIS COMPONENT

FIG. 3

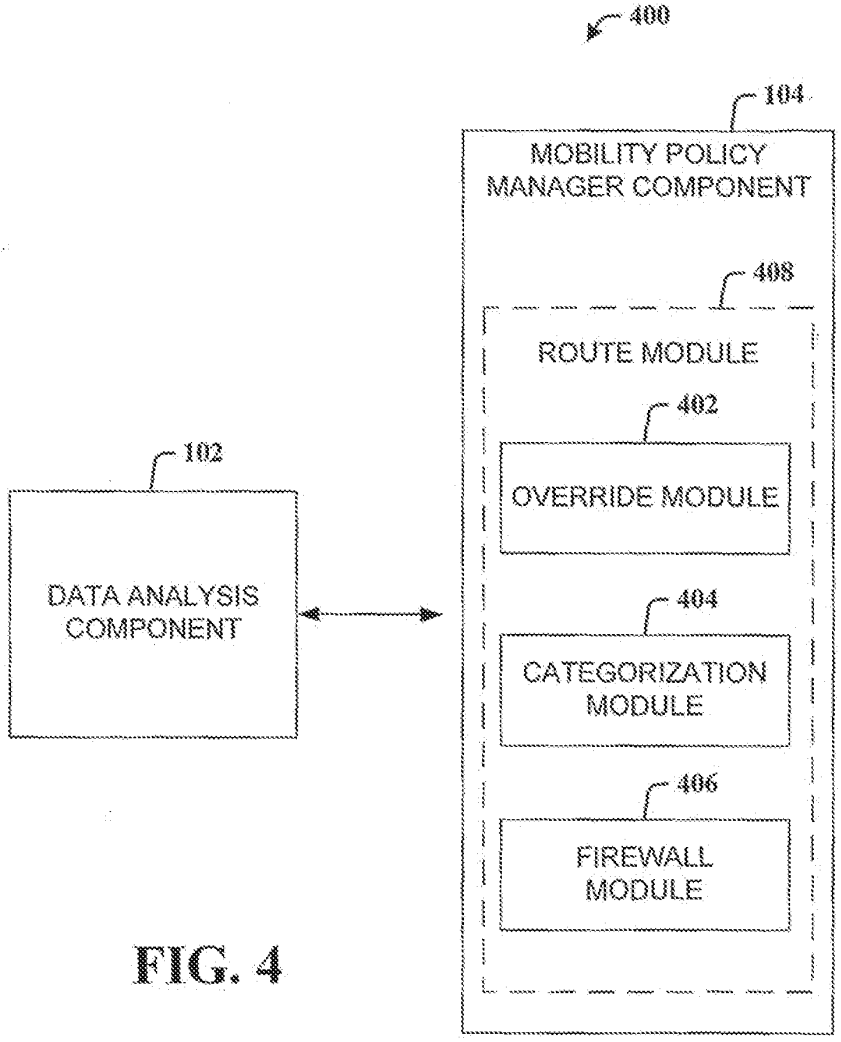

400
104
MOBILITY POLICY MANAGER COMPONENT
408
ROUTE MODULE
402
OVERRIDE MODULE
404
CATEGORIZATION MODULE
406
FIREWALL MODULE
102
DATA ANALYSIS COMPONENT

FIG. 4

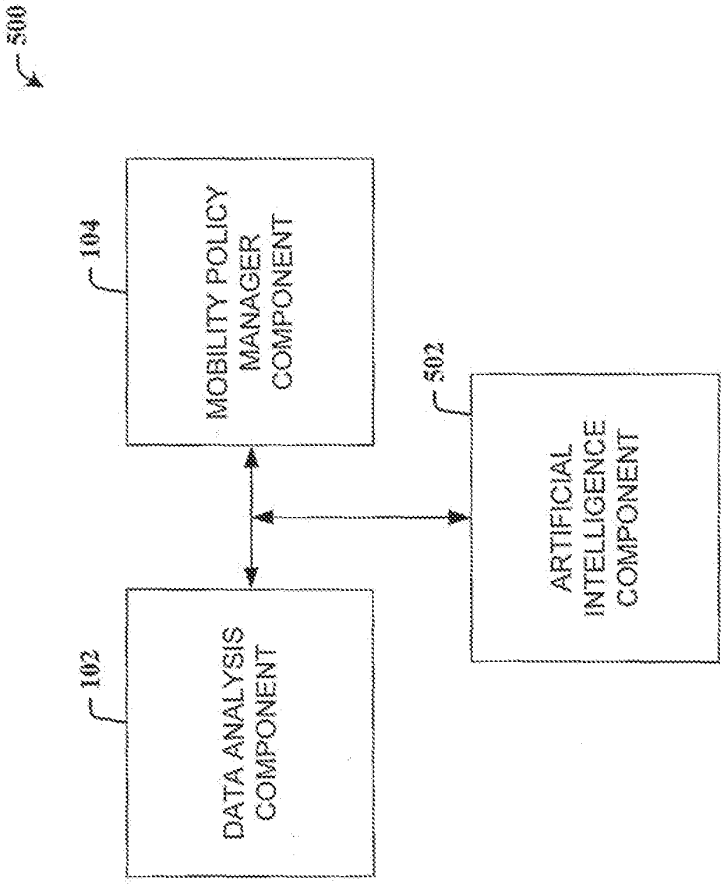

500
104
MOBILITY POLICY MANAGER COMPONENT
502
ARTIFICIAL INTELLIGENCE COMPONENT
102
DATA ANALYSIS COMPONENT

FIG. 5

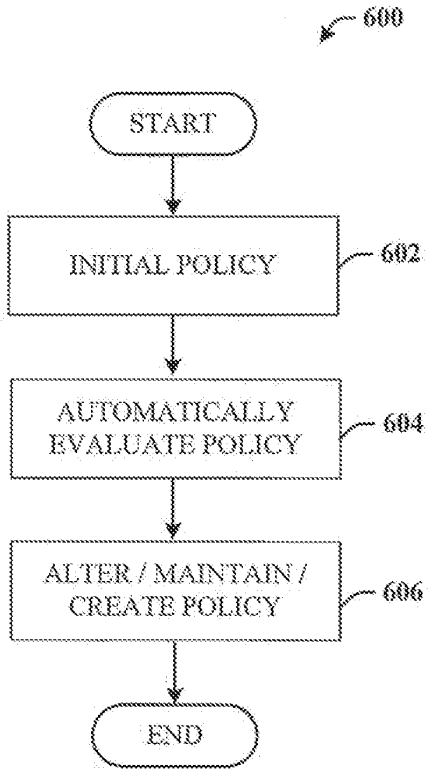

600
START
INITIAL POLICY
602
AUTOMATICALLY EVALUATE POLICY
604
ALTER / MAINTAIN / CREATE POLICY
606
END

FIG. 6

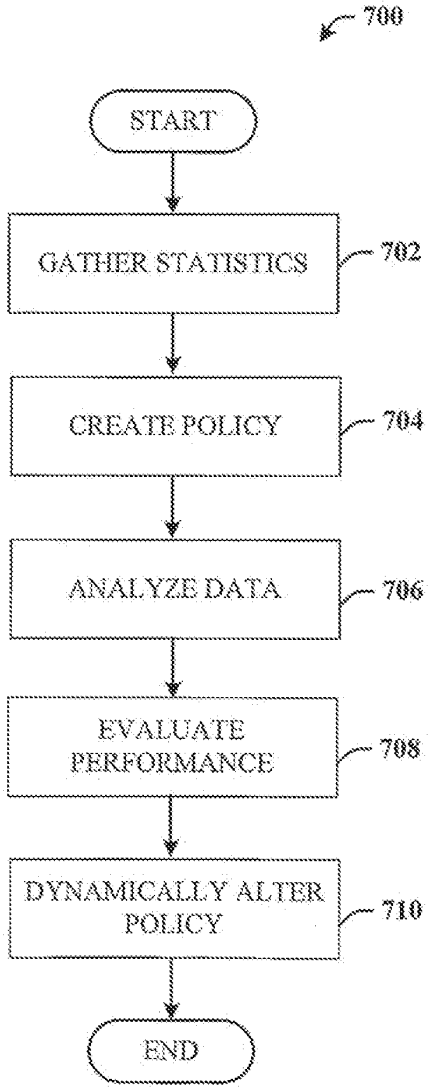

700
START
GATHER STATISTICS
702
CREATE POLICY
704
ANALYZE DATA
706
EVALUATE PERFORMANCE
708
DYNAMICALLY ALTER POLICY
710
END

FIG. 7

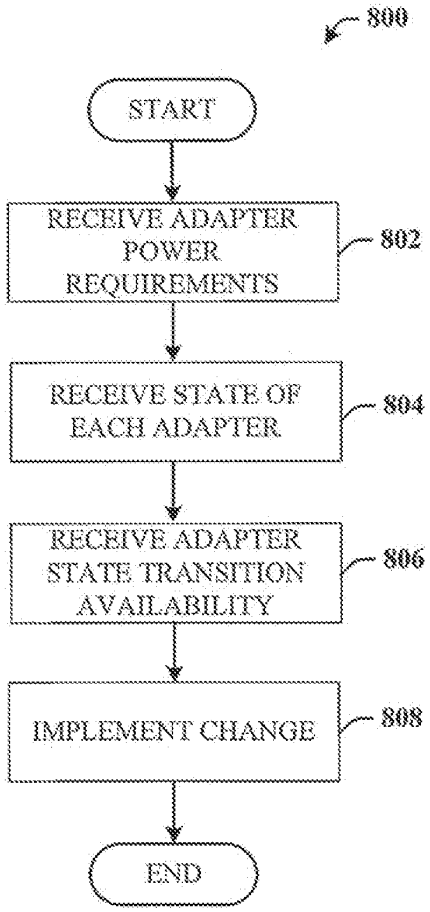

800
START
RECEIVE ADAPTER POWER REQUIREMENTS
802
RECEIVE STATE OF EACH ADAPTER
804
RECEIVE ADAPTER STATE TRANSITION AVAILABILITY
806
IMPLEMENT CHANGE
808
END

FIG. 8

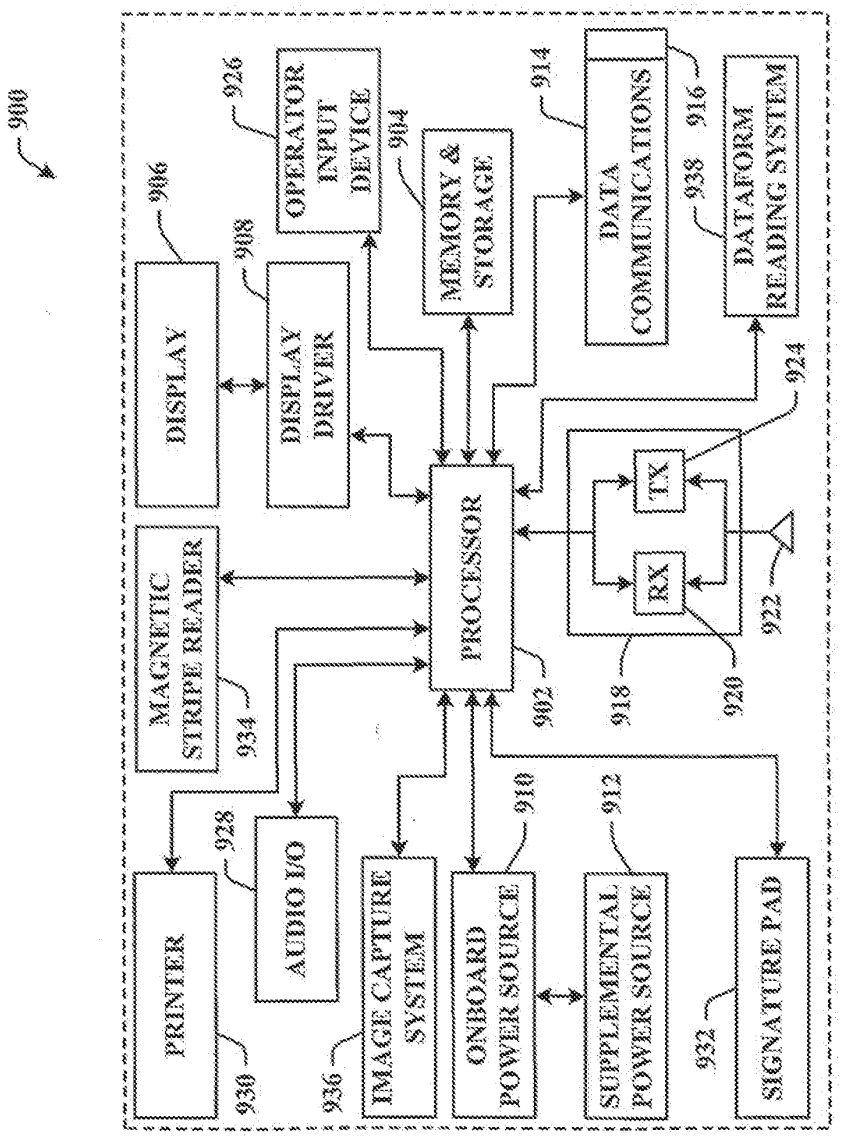

900
PRINTER
930
928
AUDIO I/O
936
IMAGE CAPTURE SYSTEM
ONBOARD POWER SOURCE
910
SUPPLEMENTAL POWER SOURCE
912
932
SIGNATURE PAD
MAGNETIC STRIPE READER
934
DISPLAY
906
908
DISPLAY DRIVER
926
OPERATOR INPUT DEVICE
904
MEMORY & STORAGE
PROCESSOR
902
914
DATA COMMUNICATIONS
938
916
DATAFORM READING SYSTEM
RX
TX
918
920
922
924

FIG. 9

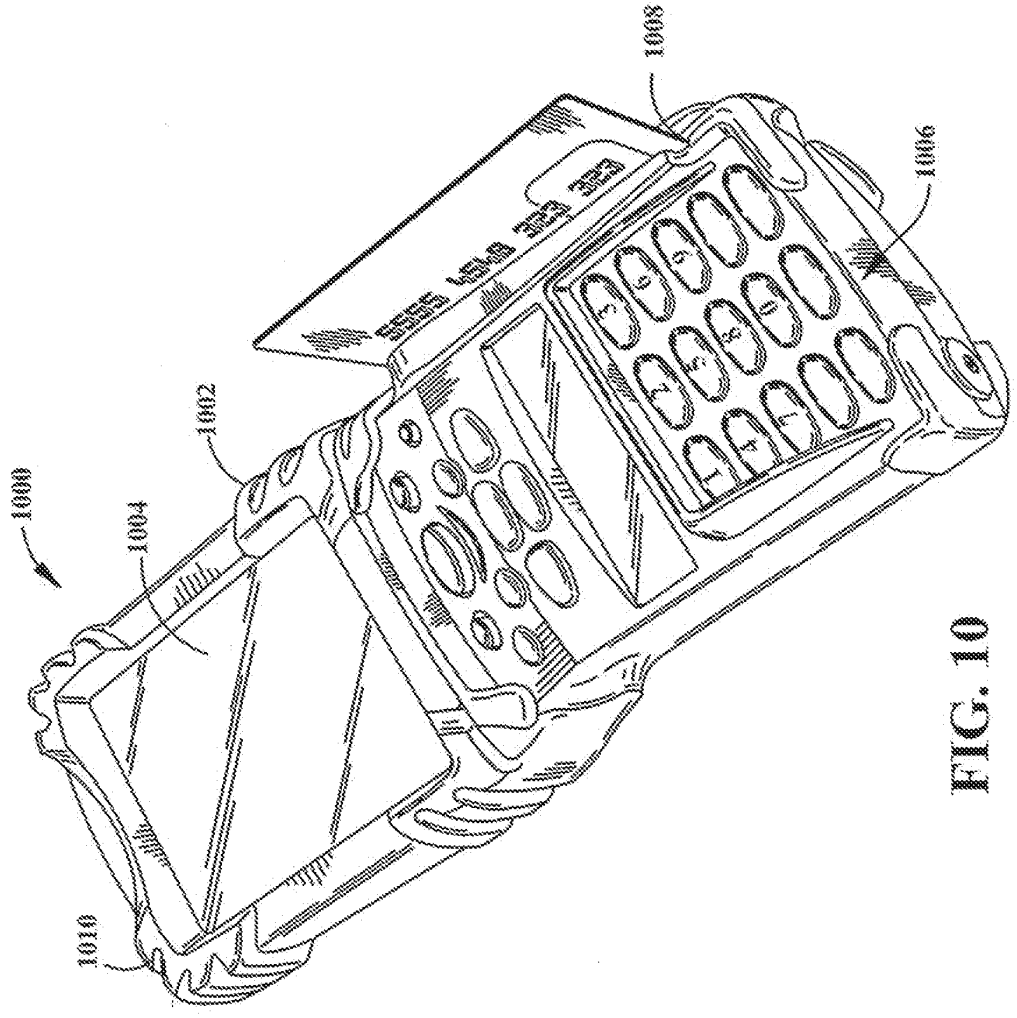


FIG. 10

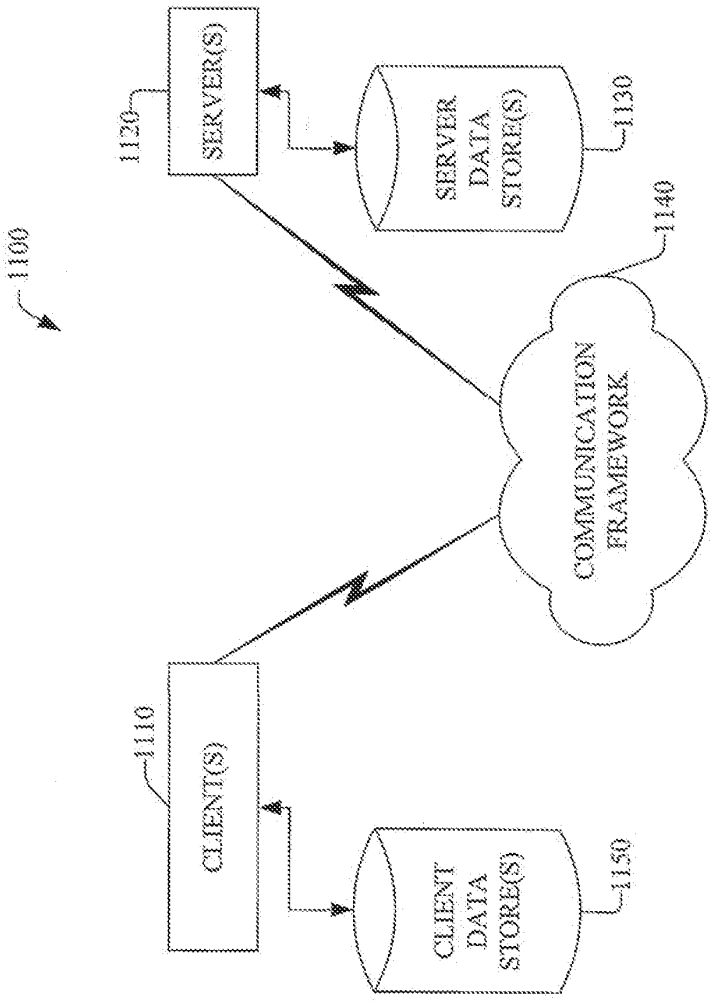

1100
1120
SERVER(S)
SERVER DATA STORE(S)
1130
1140
COMMUNICATION FRAMEWORK
1110
CLIENT(S)
CLIENT DATA STORE(S)
1150

FIG. 11

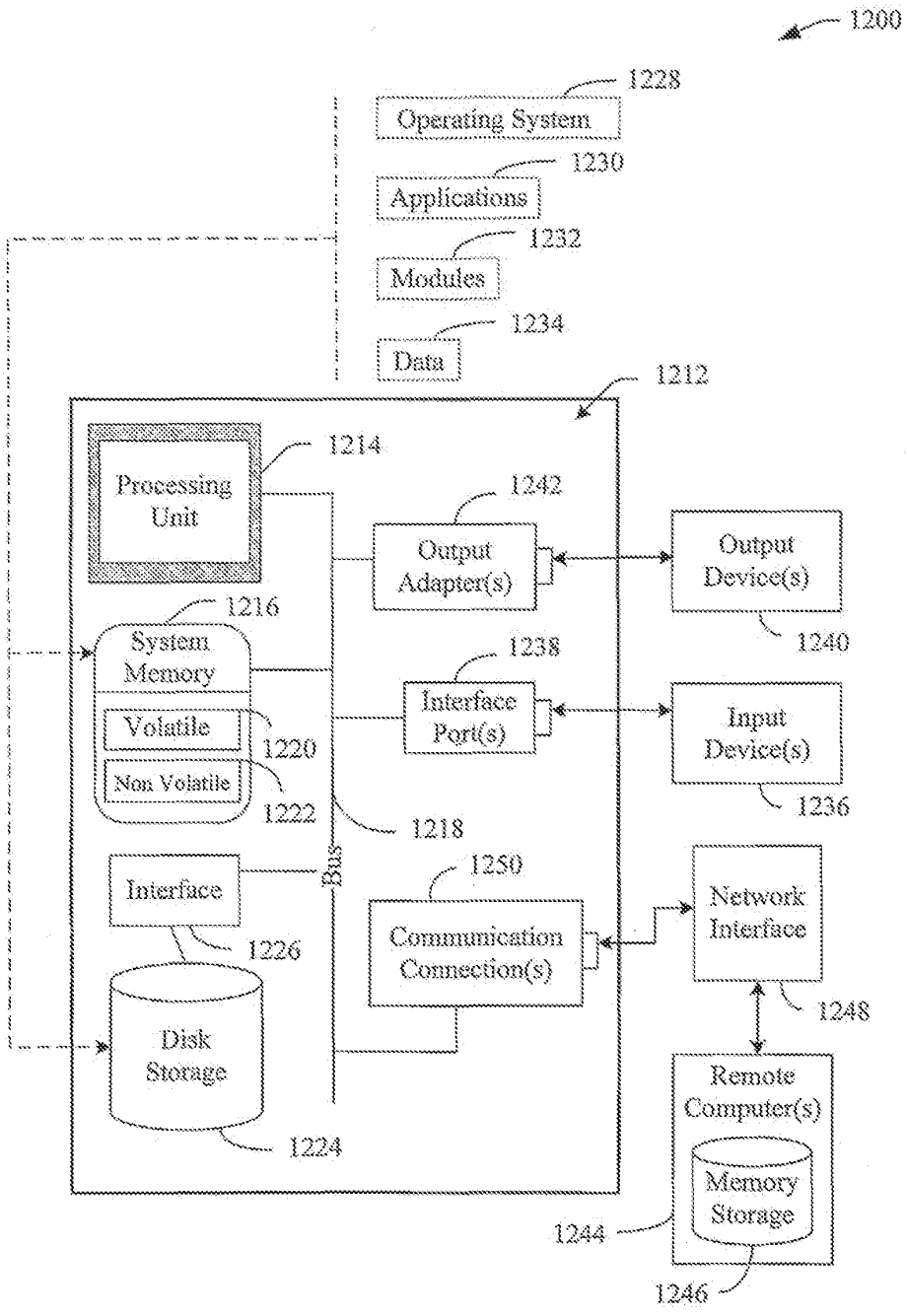

1200
1228
Operating System
1230
Applications
1232
Modules
1234
Data
1212
1214
Processing Unit
1242
Output Adapter(s)
Output Device(s)
1240
1216
System Memory
Volatile
1220
Non Volatile
1222
1238
Interface Port(s)
Input Device(s)
1236
1218
Bus
Interface
1226
1250
Communication Connection(s)
Network Interface
1248
Disk Storage
1224
Remote Computer(s)
Memory Storage
1244
1246

FIG. 12

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 739 518 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.01.2007 Bulletin 2007/01

(51) Int Cl.:
G06F 1/00 *(2006.01)*

(21) Application number: **05254068.9**

(22) Date of filing: **29.06.2005**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR LV MK YU

(71) Applicant: **Research In Motion Limited**
Waterloo, Ontario N2L 3W8 (CA)

(72) Inventors:
- **Adams, Neil P.**
  Waterloo
  Ontario N2K 4E4 (CA)
- **Little, Herbert A.**
  Waterloo
  Ontario N2T 2V8 (CA)

(74) Representative: **Roberts, Gwilym Vaughan et al**
Kilburn & Strode
20 Red Lion Street
London WC1R 4JP (GB)

(54) System and method for privilege management and revocation

(57) The present disclosure relates generally to the management of privileges associated with certain applications that are accessible by users of electronic equipment, such as, for example, networked computers, mobile wireless communications devices, and the like. In particular, the disclosure is directed to systems and methods for managing privileges associated with particular applications and for revoking these privileges in a timely and robust manner. For example, the device keeps track of which applications get access to which privileges. When policies or application control changes, the system detects which privileges have been revoked for which applications. This can be accomplished by simply comparing the old set of privileges with the new set of privileges. For each revoked privilege for a given application, the system determiner if the application has ever accessed that privilege in the past. If an application has accessed a privilege that is now revoked at any time in the past, the device is reset. To ensure that privileges that may be passed between applications are not overlooked, the device is arranged to perform a reset if any revoked privilege accessible by the device is one that may be passed between applications.

EP 1 739 518 A1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND

1. Field of the Invention

[0001] The present invention relates generally to the management of privileges associated with certain applications that are accessible by users of electronic equipment, such as, for example, networked computers, mobile wireless communications devices, and the like. In particular, the disclosure is directed to systems and methods for managing privileges associated with particular applications and for revoking these privileges in a timely and robust manner.

2. Related Art

[0002] It is well known that certain electronic equipment, such as, for example, networked computers, mobile wireless communications devices, and the like, include applications resident on such equipment that may have access to certain privileges that enable the applications to perform various functions. Typically, a system administrator may use IT policy and application control to set the privileges associated with various applications present on the equipment that is subject to the administrator's control. Examples of privileges may include, for example, allowing an application to use inter-process communication (IPC), enabling the opening of internal and external connections, enabling the injection of browser filters, enabling Bluetooth ™ functionality, enabling use of e-mail, enabling the use of personal information management (PIM) functionality, use of application program interface (API), etc. It is important for the system administrator be able to track which applications have access to which privileges, and to be able to revoke privileges on an as needed basis.

[0003] For example, if an application has access to a privilege, and the system administrator revokes that privilege, the application should immediately, or within a small window of time, be denied access to that privilege. In other words, the privilege should be revoked as soon as possible. Events that might trigger a revocation of privileges may include, for example, an application being loaded before the IT administrator/application control data is present on the device, an application is discovered to be a rogue application, or company policy changes, resulting in limiting the use or availability of certain applications and/or privileges associated therewith.

[0004] Regardless of the reason for privilege revocation, such revocation must be accomplished in a secure manner and in a manner that prevents possible work arounds by malicious applications or individuals. In general, according to current privilege revocation schemes, privilege checking is typically performed on the first access to a privilege. For example, applications communicate with IPC using the application registry. Once an application has a reference (e.g., pointer) to the application registry, it is difficult to take this reference away from the application. In another example, if an application has passed some if its privileges to another application using IPC, conventional systems can detect that the first application has access to IPC, but there is no way to detect that the other application has been passed the privilege (s).

[0005] Therefore, there remains a need for a system and method for effectively managing privileges associated with applications, and in particular, when privilege revocation is required, to revoke these privileges in a timely and robust manner.

SUMMARY

[0006] In view of the foregoing, we have now identified an efficient, accurate, robust and easy to imaplement system and method for managing privileges associated with particular applications and for revoking these privileges in a timely and reliable manner

[0007] According to an exemplary embodiment an application having privileges that are to be revoked may be shut down. When this application is restarted, access to revoked privileges will be denied. In order to keep track of which applications need to be shut down and reset, the system must keep track of which applications have accessed which privileges. To enable monitoring of the privileges accessed by applications, each time an application uses a privilege, the system records the application identifier and which privilege has been accessed. This may be done in any of a number of conventional methods, such as, for example, a data table listing the application identifier and corresponding accessed privilege(s) associated with the application identifier. When the system administrator, or any other authority, institutes a change in privileges, the system accesses the record of which applications have accessed which privileges. A comparison of accessed privileges with the privileges to be revoked is performed. Each application that has accessed a privilege that is to be revoked is identified by the system and then shut down. When the application is restarted, the application will not have access to any of the revoked privileges.

[0008] In another embodiment, a device reset may be performed. By resetting a device, the system is brought to a known state. According to this embodiment, a system administrator, or any other authority, specifies that a device must be reset when a new policy that revokes (or changes) privileges is instituted. A device reset may be instituted at any time the administrator or authority deems it necessary to do so. For example, a device reset may be done whenever a new policy that includes privilege revocation is instituted. However, this may result in numerous unnecessary device reset events that are potentially inconvenient to the user and may interfere with use of the device. Alternatively, the system may keep track of which devices include which applications, and use this

information to determine a less intrusive device reset schedule. For example, resetting only those devices having applications that may potentially be affected by the policy change.

[0009] In yet another advantageous embodiment, aspects of previously described embodiments are combined to provide effective privilege management and revocation. According to this exemplary embodiment, the system administrator or other authority has no actual control over when a device is reset. The administrator merely manages the privileges of the system and particular applications. The device itself is responsible for resetting when necessary. In this embodiment, the device keeps track of which applications get access to which privileges. When policies or application control changes, the system detects which privileges have been revoked for which applications. This can be accomplished by simply comparing the old set of privileges with the new set of privileges. For each revoked privilege for a given application, the system determines if the application has ever accessed that privilege in the past. As noted above, the system has been keeping track of these since the system was first started up. If an application has accessed a privilege that is now revoked at any time in the past, the device is reset. For some privileges (e.g., IPC), it still cannot be determined whether a privilege has been used as a result of being passed from another application. To overcome the potential for missing a revocation of privileges when applications pass privileges between themselves, if, for example, IPC (or any other privilege that is able to be passed between applications) is revoked from any application, regardless of if the system has detected that the application has accessed the privilege, the device must be reset. This reset will bring the device back to a known state. Device reset will only be done when necessary, thus limiting the number of resets and solving the problem associated with privileges that have been passed between applications.

[0010] Each of these embodiments is useful in a variety of privilege management environments ranging from a low-level low-priority where a modest level of privilege revocation security is needed, resulting in a less robust system, to a highly important ultra-robust environment where user inconvenience is secondary to the need for absolute certainty of privilege revocation.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] These and other embodiments along with their attendant advantages are described herein with reference to the following drawings in which like reference numerals refer to like elements, and wherein:

FIG. 1 is a block diagram showing a computer network and communication system in which electronic devices running applications having access to associated privileges are used;

FIG. 2 is a block diagram of a wireless mobile communication device as an example of an electronic device running applications having access to associated privileges;

FIG. 3 is a flow diagram illustrating a method of revoking privileges according to an exemplary embodiment;

FIG. 4 is a flow diagram illustrating a method of revoking privileges according to another exemplary embodiment; and

FIG. 5 is a flow diagram illustrating yet another method of revoking privileges according to another exemplary embodiment.

DETAILED DESCREMON OF EXEMPLARY EMBODIMENTS

[0012] FIG. 1 is a block diagram showing a computer network and communication system in which electronic devices running applications having access to associated privileges are uses. The computer network 18 includes, for example, various networked computers 28 and, optionally, a message server 26, all linked via a Local Area Network (LAN) 30. The communication system includes a Wide Area Network (WAN) 12 coupled to a computer system 14, a wireless network gateway 16 and the LAN 30 of the computer network 18. The wireless network gateway 16 is also connected to a wireless communication network 20 in which a wireless mobile communication device 22 (hereinafter "mobile device"), is configured to operate. The entire system 10 is typically managed by, among others, a system administrator or like authority 32.

[0013] The computer system 14 may be a desktop or laptop personal computer that is configured to communicate with the WAN 12 or any other suitable network, such as, for example, the Internet. Personal computers, such as the computer system 14, typically access the Internet via an Internet Service Provider (ISP), Application Service Provider (ASP),or the like.

[0014] The LAN 30 is an example of a typical working computer network environment, in which multiple computers 28 are connected in a network. The computer network 18 is typically located behind a security firewall 24. Within the LAN 30, a message server 26, operating on a computer behind the firewall 24 may act as the primary interface for the owner of the computer network 18 to exchange messages both within the LAN 30 and with other external messaging clients via the WAN 12. Known message servers include, for example, Microsoft Outlook™, Lotus Notes™, Yahoo!™ Messenger, AOL Instant Messenger, or any other client-server or peer-to-peer, or similar messaging clients with various architectures. Messages received by the message server 26 are distributed to mailboxes for user accounts addressed in

the received messages, and are then accessed by a user through a messaging client operating on a computer system 28. The foregoing is merely an exemplary description illustrating a client-server architecture, and in no way implies that such architecture is necessary, as other suitable architectures known to those skilled in the art may be used.

[0015] Although only a message server 26 is shown in the LAN 30, those skilled in the art will appreciate that a LAN may include other types of servers supporting resources that are shared between the networked computer systems 28, and that the message server 26 may also provide additional functionality, such as dynamic database storage for data such as, but not limited to, calendars, to-do lists, task lists, e-mail and documentation. The message server 26 and electronic messaging are described for illustrative purposes only. Systems and methods for managing and revoking privileges are applicable to a wide range of electronic devices, and are in no way limited to electronic devices with messaging capabilities.

[0016] The wireless gateway 16 provides an interface to a wireless network 20. through which messages may be exchanged with a mobile device 22. Such functions as addressing of the mobile device 22, encoding or otherwise transforming messages for wireless transmission, and any other interface functions are performed by the wireless gateway 16. The wireless gateway 16 may be configured to operate with more than one wireless network 20, in which case the wireless gateway 16 also determines a most likely network for locating a given mobile device 22 and possibly track mobile devices as users roam between countries or networks.

[0017] The mobile device 22 is, for example, a data communication device, a voice communication device, a dual-mode communication device such as many modem cellular telephones having both data and voice communications functionality, a multiple-mode device capable of voice, data and other types of communications, a personal digital assistant (PDA) enabled for wireless communications, or a laptop or desktop computer system with a wireless modem.

[0018] Any computer system with access to the WAN 12 may exchange messages with the mobile device 22 through the wireless network gateway 16. Alternatively, private wireless network gateways such as wireless Virtual Private Network (VPN) routers could be implemented to provide a private interface to a wireless network. A wireless VPN router implemented in the LAN 30 provides a private interface from the LAN 30 to one or more mobile devices such as 22 through the wireless network 20. A private interface to a mobile device 22 may also effectively be extended to entities outside the LAN 30 by providing a message forwarding or redirection system that operates with the message server 26. Such a message redirection system is disclosed in United States Patent No. 6,219,694, which is hereby incorporated into this application by reference. In this type of system, incoming messages received by the message server 26 and addressed to a user of a mobile device 22 are sent through the wireless network interface, either a wireless VPN router, the wireless gateway 16, or another interface, for example, to the wireless network 20 and to the user's mobile device 22. Another alternate interface to a user's mailbox on a message server 26 may be a Wireless Application Protocol (WAP) gateway. Through a WAP gateway, a list of messages in a user's mailbox on the message server 26, and possibly each message or a portion of each message, may be sent to the mobile device 22. A wireless network 20 normally delivers messages to and from communication devices such as the mobile device 22 via RF transmissions between base stations and devices. The wireless network 20 may, for example, be a data-centric wireless network, a voice-centric wireless network, or a dual-mode network that can support both voice and data communications over the same infrastructure. Recently developed networks include Code Division Multiple Access (GDMA) networks and General Packet Radio Service (GPRS) networks. So-called third-generation (3G) networks like Enhanced Data rates for Global Evolution (EDGE) and Universal Mobile Telecommunications Systems (UMTS) are currently under development. Older data-centric networks include, but are not limited to, the Mobitex™ Radio Network ("Mobitex"), and the DataTAC™ Radio Network ("DataTAC"). Voice-centric data networks such as Personal Communication System (PCS) networks, including Global System for Mobile Communications (GSM) and Time Division Multiple Access (TDMA) systems, have been available in North America and world-wide for several years.

[0019] FIG. 2 is a block diagram of an exemplary wireless mobile communication device as an example of an electronic device. However, it should be understood that the systems and methods disclosed herein may be used with many different types of devices, such as personal digital assistants (PDAs), desktop computers, or the like.

[0020] The mobile device 500 is preferably a two-way communication device having at least voice and data communication capabilities. The mobile device 500 preferably has the capability to communicate with other computer systems on the Internet. Depending on the firnctionality provided by the mobile device, the mobile device may be referred to as a data messaging device, a two-way pager, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device (with or without telephony capabilities). As mentioned above, such devices are refened to generally herein as mobile devices.

[0021] The mobile device 500 includes a transceiver 511, a microprocessor 538, a display 522, non-volatile memory 524, random access memory (RAM) 526, auxiliary input/output (I/O) devices 528, a serial port 530, a keyboard 532, a speaker 534, a microphone 536, a short-range wireless communications subsystem 540, and may also include other device sub-systems 542. The transceiver 511 preferably includes transmit and receive

antennas 516, 518, a receiver (Rx) 512, a transmitter (Tx) 514, one or more local oscillators (LOs) 513, and a digital signal processor (DSP) 520. Within the non-volatile memory 524, the mobile device 500 includes a plurality of software modules 524A-524N that can be executed by the microprocessor 538 (and/or the DSP 520), including a voice communication module 524A, a data communication module 524B, and a plurality of other operational modules 524N for carrying out a plurality of other functions.

[0022] The mobile device 500 is preferably a two-way communication device having voice and data communication capabilities. Thus, for example, the mobile device 500 may communicate over a voice network, such as any of the analog or digital cellular networks, and may also communicate over a data network. The voice and data networks are depicted in FIG. 2 by the communication tower 519. These voice and data networks may be separate communication networks using separate infrastructure, such as base stations, network controllers, etc., or they may be integrated into a single wireless network. References to the network 519 should therefore be interpreted as encompassing both a single voice and data network and separate networks.

[0023] The communication subsystem 511 is used to communicate with the network 519. The DSP 520 is used to send and receive communication signals to and from the transmitter 514 and receiver 512, and also exchange control information with the transmitter 514 and receiver 512. If the voice and data communications occur at a single frequency, or closely-spaced set of frequencies, then a single LO 513 may be used in conjunction with the transmitter 514 and receiver 512. Alternatively, if different frequencies are utilized for voice communications versus data communications or the mobile device 500 is enabled for communications on more than one network 519, then a plurality of LOs 513 can be used to generate frequencies corresponding to those used in the network 519. Although two antennas 516, 518 are depicted in FIG. 2, the mobile device 500 could be used with a single antenna structure. Information, which includes both voice and data information, is communicated to and from the communication module 511 via a link between the DSP 520 and the microprocessor 538,

[0024] The detailed design of the communication subsystem 511, such as frequency band, component selection, power level, etc., is dependent upon the communication network 519 in which the mobile device 500 is intended to operate. For example, a mobile device 500 intended to operate in a North American market may include a communication subsystem 511 designed to operate with the Mobitex or DataTAC mobile data communication networks and also designed to operate with any of a variety of voice communication networks, such as AMPS, TDMA, CDMA, PCS, etc., whereas a mobile device 500 intended for use in Europe may be configured to operate with the GPRS data communication network and the GSM voice communication network. Other types of data and voice networks, both separate and integrated, may also be utilized with the mobile device 500.

[0025] Communication network access requirements for the mobile device 500 also vary depending upon the type of network 519. For example, in the Mobitex and DataTAC data networks, mobile devices are registered on the network using a unique identification number associated with each device. In GPRS data networks, however, network access is associated with a subscriber or user of the mobile device 500. A GPRS device typically requires a subscriber identity module ("SIM"), which is required in order to operate the mobile device 500 on a GPRS network. Local or non-network communication functions (if any) may be operable, without the SIM, but the mobile device 500 is unable to carry out functions involving communications over the network 519, other than any legally required operations, such as '911' emergency calling.

[0026] After any required network registration or activation procedures have been completed, the mobile device 500 is able to send and receive communication signals, preferably including both voice and data signals, over the network 519. Signals received by the antenna 516 from the communication network 519 are routed to the receiver 512, which provides for signal amplification, frequency down conversion, filtering, channel selection, etc., and may also provide analog to digital conversion. Analog to digital conversion of the received signal allows more complex communication functions, such as digital demodulation and decoding, to be performed using the DSP 520. In a similar manner, signals to be transmitted to the network 519 are processed, including modulation and encoding, for example, by the DSP 520 and are then provided to the transmitter 514 for digital to analog conversion, frequency up conversion, filtering, amplification and transmission to the communication network 519 via the antenna 518. Although a single transceiver 511 is shown for both voice and data communications, in alternative embodiments, the mobile device 500 may include multiple distinct transceivers, such as a first transceiver for transmitting and receiving voice signals, and a second transceiver for transmitting and receiving data signals, or a first transceiver configured to operate within a first frequency band, and a second transceiver configured to operate within a second frequency band.

[0027] In addition to processing the communication signals, the DSP 520 also provides for receiver and transmitter control. For example, the gain levels applied to communication signals in the receiver 512 and transmitter 514 may be adaptively controlled through automatic gain control algorithms implemented in the DSP 520. Other transceiver control algorithms could also be implemented in the DSP 520 in order to provide more sophisticated control of the transceiver 511.

[0028] The microprocessor 538 preferably manages and controls the overall operation of the mobile device 500. Many types of microprocessors or microcontrollers could be used here, or, alternatively, a single DSP 520

could be used to carry out the functions of the microprocessor 538. Low-level communication functions, including at least data and voice communications, are performed through the DSP 520 in the transceiver 511. High-level communication applications, including the voice communication application 524A, and the data communication application 524B are stored in the non-volatile memory 524 for execution by the microprocessor 538. For example, the voice communication module 524A may provide a high-level user interface operable to transmit and receive voice calls between the mobile device 500 and a plurality of other voice devices via the network 519. Similarly, the data communication module 524B may provide a high-level user interface operable for sending and receiving data, such as e-mail messages, files, organizer information, short text messages, etc., between the mobile device 500 and a plurality of other data devices via the network 519.

[0029] The microprocessor 538 also interacts with other device subsystems, such as the display 522, RAM 526, auxiliary I/O devices 528, serial port 530, keyboard 532, speaker 534, microphone 536, a short-range communications subsystem 540 and any other device subsystems generally designated as 542. For example, the modules 524A-N are executed by the microprocessor 538 and may provide a high-level interface between a user of the mobile device and the mobile device. This interface typically includes a graphical component provided through the display 522, and an input/output component provided through the auxiliary I/O devices 528, keyboard 532, speaker 534, or microphone 536. Additionally, the microprocessor 538 is capable of running a variety of applications that may be present in the device non-volatile memory 524, including applications that have access to various privileges, as will be described in more detail herein.

[0030] Some of the subsystems shown in FIG. 2 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 532 and display 522 may be used for both communication-related functions, such as entering a text message for transmission over a data communication network, and device-resident functions such as a calculator or task list or other PDA type functions.

[0031] Operating system software used by the microprocessor 538 is preferably stored in a persistent store such as the non-volatile memory 524. In addition to the operating system and communication modules 524A-N, the non-volatile memory 524 may include a file system for storing data. The non-volatile memory 524 may also include data stores for owner information and owner control information. The operating system, specific device applications or modules, or parts thereof, may be temporarily loaded into a volatile store, such as RAM 526 for faster operation. Moreover, received communication signals may also be temporarily stored to RAM 526, before permanently writing them to a file system located in the non-volatile memory 524. The non-volatile memory 524 may be implemented, for example, with Flash memory, non-volatile RAM, or battery backed-up RAM.

[0032] An exemplary application module 524N that may be loaded onto the mobile device 500 is a PIM application providing PDA functionality, such as calendar events, appointments, and task items. This module 524N may also interact with the voice communication module 524A for managing phone calls, voice mails, etc., and may also interact with the data communication module 524B for managing e-mail communications and other data transmissions. Alternatively, all of the functionality of the voice communication module 524A and the data communication module 524B may be integrated into the PIM module.

[0033] The non-volatile memory 524 preferably provides a file system to facilitate storage of PIM data items on the device. The PIM application preferably includes the ability to send and receive data items, either by itself, or in conjunction with the voice and data communication modules 524A, 524B, via the wireless network 519. The PIM data items are preferably seamlessly integrated, synchronized and updated, via the wireless network 519, with a corresponding set of data items stored or associated with a host computer system, thereby creating a mirrored system for data items associated with a particular user.

[0034] The mobile device 500 is manually synchronized with a host system by placing the mobile device 500 in an interface cradle, which couples the serial port 530 of the mobile device 500 to a serial port of the host system. The serial port 530 may also be used to insert owner information and owner control information onto the mobile device 500 and to download other application modules 524N for installation on the mobile device 500. This wired download path may further be used to load an encryption key onto the mobile device 500 for use in secure communications, which is a more secure method than exchanging encryption information via the wireless network 519.

[0035] Owner information, owner control information and additional application modules 524N may be loaded onto the mobile device 500 through the network 519, through an auxiliary I/O subsystem 528, through the short-range communications subsystem 540, or through any other suitable subsystem 542, and installed by a user in the non-volatile memory 524 or RAM 526. Such flexibility in application installation increases the functionality of the mobile device 500 and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the mobile device 500.

[0036] When the mobile device 500 is operating in a data communication mode, a received signal, such as a text message or a web page download, will be processed by the transceiver 511 and provided to the microproces-

sor 538, which preferably further processes the received signal for output to the display 522, or, alternatively, to an auxiliary I/O device 528. Owner information, owner control information, commands or requests related to owner information or owner control information, and software applications received by the transceiver 511 are processed as described above. A user of mobile device 500 may also compose data items, such as email messages, using the keyboard 532, which is preferably a complete alphanumeric keyboard laid out in the QWERTY style, although other styles of complete alphanumeric keyboards such as the known DVORAK style may also be used. User input to the mobile device 500 is further enhanced with the plurality of auxiliary I/O devices 528, which may include a thumbwheel input device, a touchpad, a variety of switches, a rocker input switch, etc. The composed data items input by the user are then transmitted over the commuaication network 519 via the transceiver 511.

[0037] When the mobile device 500 is operating in a voice communication mode, the overall operation of the mobile device 500 is substantially similar to the data mode, except that received signals are output to the speaker 534 and voice signals for transmission are generated by a microphone 536. In addition, the secure messaging techniques described above might not necessarily be applied to voice communications. Alternative voice or audio I/O devices, such as a voice message recording subsystem, may also be implemented on the mobile device 500. Although voice or audio signal output is accomplished through the speaker 534, the display 522 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information. For example, the microprocessor 538, in conjunction with the voice communication module 524A and the operating system software, may detect the caller identification information of an incoming voice call and display it on the display 522.

[0038] A short-range communications subsystem 540 is also be included in the mobile device 500. For example, the subsystem 540 may include an infrared device and associated circuits and components, or a Bluetooth or 802.11 short-range wireless communication module to provide for communication with similarly-enabled systems and devices. Thus, owner information insertion, owner control information insertion, and application loading operations as described above may be enabled on the mobile device 500 via the serial port 530 or other short-range communications subsystem 540.

[0039] FIG. 2 represents a specific example of an electronic device in which owner control systems and methods described herein may be implemented. Implementation of such systems and methods in other electronic devices having further, fewer, or different components than those shown in FIG. 2 would occur to one skilled in the art to which this application pertains and are therefore considered to be within the scope of the present application.

[0040] FIG. 3 is a flow diagram illustrating a method of revoking privileges according to an exemplary embodiment. In this example, an application having privileges that are to be revoked may be shut down. When the application is restarted, access to revoked privileges will be denied. In order to keep track of which applications need to be shut down and reset, the system must keep track of which applications have access to which privileges. To accomplish this, for example, the system monitors and detects use of privileges by applications 300. The system may record an application identifier associated with a particular application and which privilege has been accessed by the application 302. This may be accomplished in any number of conventional methods that are readily apparent to those skilled in the art. For example, a data table listing the application identifier and having pointers directed to privilege(s) accessed by the application or associated with the application identifier. The system then continues to monitor the system for any change, for example, a change in IT policy, that might result in a revocation of privileges 304. So long as no such change is detected in decision block 304, the system continues to monitor and keep track of applications and associated privileges.

[0041] Upon a detection of a change that would result in revocation of privileges being accessed by applications in the system by the decision block 304, such as, for example, a change in IT policy, a comparison of the recorded data relating to the accessed privileges with a listing of the new privileges is performed 306. For example, the application identifiers and associated accessed privileges recorded in step 302 are compared to the new privilege list, or to a list of revoked privileges 306. The changes discussed herein are typically instituted and administered by a system administrator or other authority who has responsibility for operation and management of the system.

[0042] As a result of the comparison 306, each application that has accessed a privilege(s) to be revoked is identified 308 by the system. Upon identification of these applications, the system implements a shut down of these identified applications 310. When these applications are restarted 312, the applications will not have access to any of the revoked privileges. The system will continue to monitor and detect the accessing of privileges and associated applications as described above.

[0043] In another embodiment, as illustrated in the flow diagram of FIG. 4, a device reset may be performed. According to this example, all devices in the system are monitored 400. A system administrator or other authority specifies, for example, that whenever there is a change in system policy that requires revocation or changes in privileges 402, all devices in the system must be reset 404. Resetting the devices brings the system to a known state, i.e., a state in which the system knows which applications have access to which privileges throughout the system. Upon restarting these applications 406 after the device reset 404, the applications will no longer have

access to any of the revoked privileges. According to this example, a device reset may be instituted any time the system administrator or authority deems it necessary to do so. For example, a device reset may be done whenever a new policy that includes privilege revocation is instituted. As a result, this solution may invoke numerous (potentially unnecessary) device reset events that may be intrusive and inconvenient for the users. However, this embodiment provides very robust and timely privilege revocation, and is thus suitable to highly secure systems where privilege management is more important than user convenience.

[0044] Turning now to FIG. 5, another advantageous embodiment implementing features of both embodiments described above with respect to FIGS. 3 and 4 is illustrated. According to this example, aspects of the previously described embodiments are combined to provide highly effective and timely privilege management and revocation. In this example, the system administrator or authority has no actual control over when a device is reset. The administrator or authority merely manages the privileges of the system and of particular applications. The device itself is responsible for resetting as needed.

[0045] In this example, the device monitors which applications of the device have access to which privileges 600, and a log of privileges for the device is kept 602. The device monitors whether policies or application control changes are made in the system 604. If there is no change detected 604, the device continues to monitor applications and keep a log of privileges for the device 600, 602. If a change in policy or application control is detected in step 604, the system determines which privileges have been revoked for which applications by comparing the old set of privileges in the log with the new set of privileges received from the system administrator 606. The device then determines if any revoked privileges are present on the device 608. If revoked privileges are detected, e.g., if an application has accessed a privilege at any time in the past that has now been revoked, the device will reset 610. As described above, resetting the device brings the system to a known state in which all applications and privileges are known. After the device is reset 610, it is restarted 612. Upon restart 612, the device applications will have access to the correct privileges. Advantageously, if no revoked privileges are detected in step 608, the device performs another check to ensure that no privileges that have been passed between application have been missed. As explained above, for some privileges, e.g., IPC, it cannot be determined whether a privilege has been used as a result of being passed from another application. To overcome the potential for missing revocation of privileges when applications pass privileges between themselves, the system checks for privileges that are able to be passed between applications (e.g., IPC) 614. If a privilege that is able to be passed between applications is revoked from any application, regardless of if the system has detected that the application has accessed the privilege 614, the device must be reset 610 to bring the system to a known state. After resetting, the device is restarted 612, and will now have the only have access to the correct privileges. In this manner, device reset will only be performed when necessary, thus limiting the number of resets and solving the problem associated with privileges that go undetected due to their ability to be passed between applications.

[0046] While this disclosure describes specific exemplary embodiments, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the exemplary embodiments described herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention, as defined in the following claims.

Claims

1. A method for managing privileges associated with applications in an electronic system, comprising:

   monitoring devices in the electronic system to detect use of privileges by applications being run by the device;
   recording which applications have accessed which privileges;
   detecting a change in privileges of the system;
   comparing recorded privileges previously accessed by applications with a set of privilege changes;
   identifying any privileges to be revoked based on a result of said comparing step;
   when a privilege to be revoked is identified, shutting down an application that has previously accessed the revoked privilege; and
   restarting any application that was shut down for having accessed a revoked privilege.

2. A method according to claim 1, wherein said step of recording, compnses:

   storing an application identifier associated with an application that has accessed a privilege; and
   associating said identifier with the privilege accessed by the application.

3. A method according to claim 2, wherein said recording is stored in a data table listing the application identifier and privileges associated therewith.

4. A method according to claim 1, wherein said set of privilege changes comprises privileges to be revoked.

5. A method according to claim 1, wherein said set of privilege changes comprises a listing of all privileges available for use, and does not include privileges to

be revoked.

6. A method according to claim 1, wherein said devices comprise a wireless mobile electronic communication device.

7. A method according to claim 1, further comprising continuously repeating the steps.

8. A method according to claim 1, wherein said change in privileges is a result of a change in system IT policy.

9. A method for managing privileges in a system comprising electronic devices having applications resident on said devices, comprising:

monitoring electronic devices that are present in the system;
detecting a change in privileges available to said electronic devices; and
resetting said electronic devices in response to detection of a change in privileges.

10. A method according to claim 9, wherein said change in privileges is a result of a change in system IT policy.

11. A method according to claim 9, wherein said change in privileges includes an indication that privileges are to be revoked.

12. A method according to claim 9, wherein a system administrator determines when said resetting step is performed.

13. A method according to claim 9, wherein said step of resetting said electronic devices brings said system to a known state.

14. A method according to claim 13, further comprising restarting said electronic devices after said devices have been reset.

15. A method according to claim 9, wherein said electronic devices include a mobile wireless communications device.

16. A method for managing privileges in a system comprising a plurality of electronic devices, said method comprising:

monitoring, by each device of the system, which applications on each device have access to which privileges;
recording privileges accessible via applications resident on each device of the system;
detecting a change in privileges available to said devices in said system;
comparing an old set of privileges with a new set of privileges, said new set of privileges corresponding to said change in privileges;
determining if any privileges are to be revoked based on said comparison;
resetting each device that has access to a privilege that is to be revoked;
determining whether any privileges to be revoked are able to be passed between applications; and
when a privilege to be revoked is able to be passed between applications, resetting each device that has access to said privilege.

17. A method according to claim 16, wherein said change in privileges is a result of a change in system IT policy.

18. A method according to claim 16, wherein said change in privileges includes an indication that privileges are to be revoked

19. A method according to claim 16, wherein said step of resetting said electronic devices brings said system to a known state.

20. A method according to claim 19, further comprising restarting said electronic devices after said devices have been reset.

21. A method according to claim 16, wherein said electronic devices include a mobile wireless communications device.

22. A system for managing privileges in a network comprising a plurality of electronic devices, said system comprising:

a processor resident in each device of the system, for monitoring which applications on each device have access to which privileges;
a memory for recording privileges accessible via applications resident on each device of the system; and
wherein said processor is operable to:

detect a change in privileges available to said devices in said system;
compare an old set of privileges with a new set of privileges, said new set of privileges corresponding to said change in privileges;
determine if any privileges are to be revoked based on said comparison;
reset each device that has access to a privilege that is to be revoked; and
determine whether any privileges to be revoked are able to be passed between ap-

plications, and when a privilege to be revoked is able to be passed between applications, resetting each device that has access to said privilege.

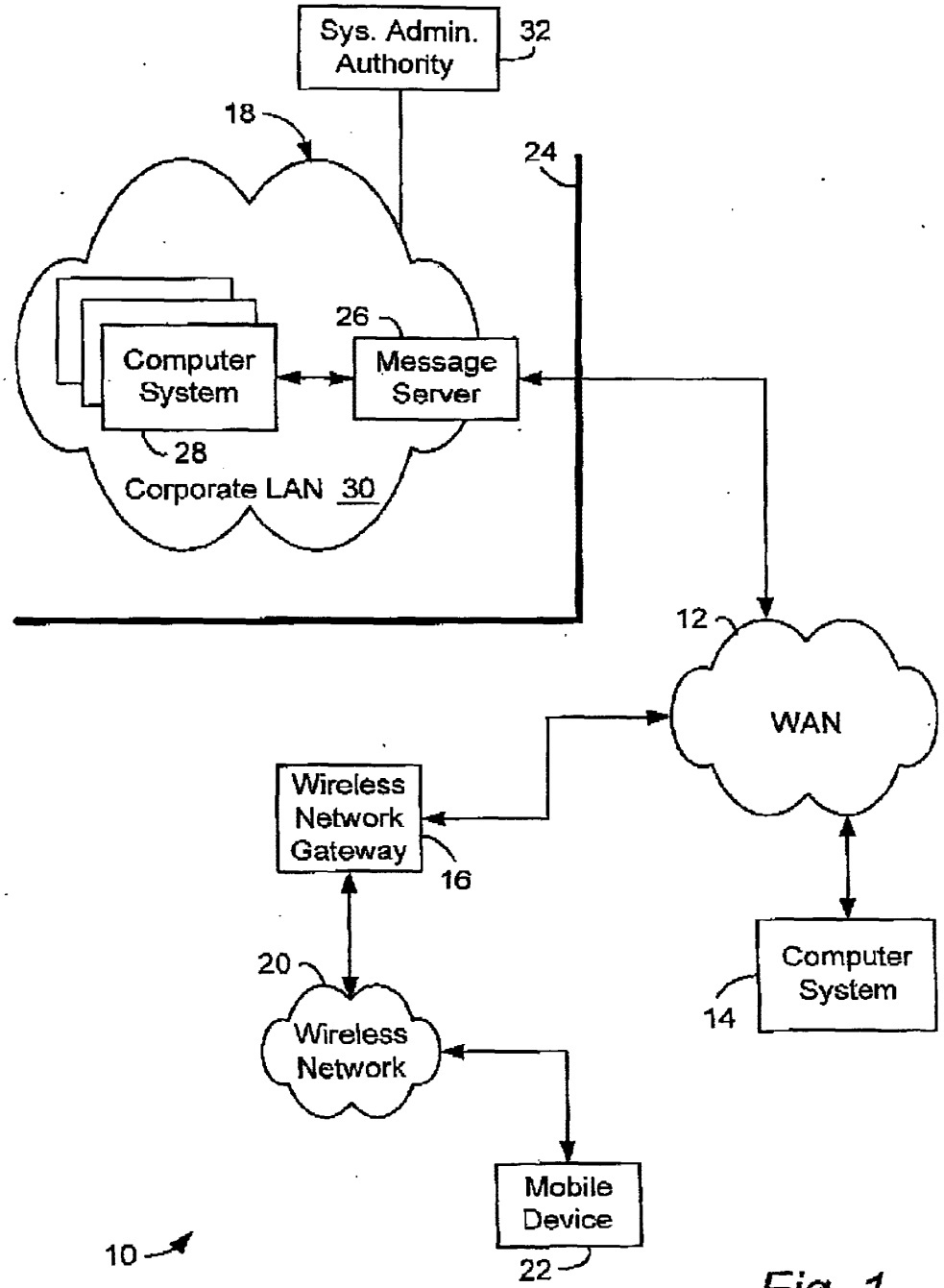

Sys. Admin. Authority
32
18
24
26
Computer System
Message Server
28
Corporate LAN 30
12
WAN
Wireless Network Gateway
16
20
Wireless Network
Computer System
14
Mobile Device
22
10

Fig. 1

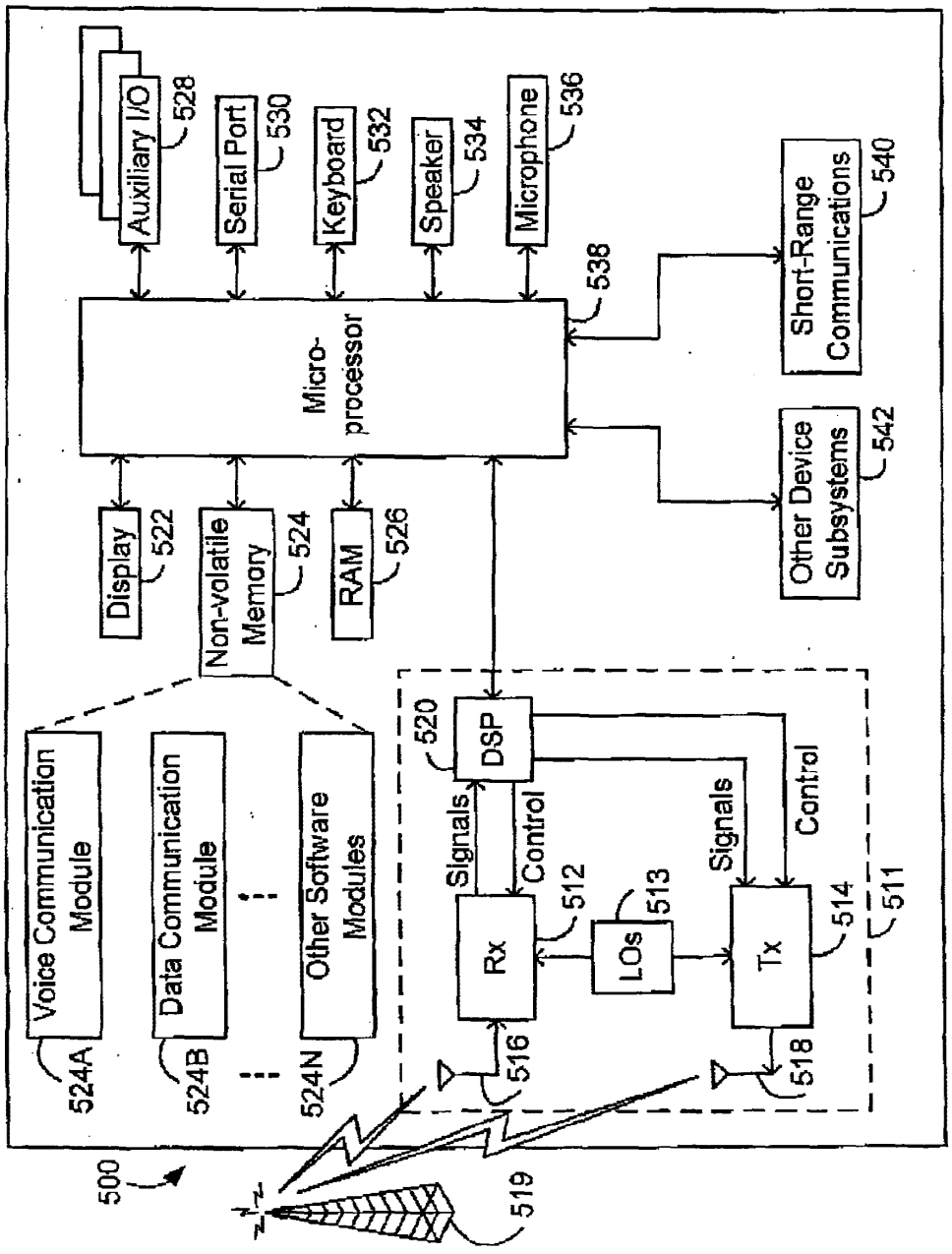

Auxiliary I/O
528
Serial Port
530
Keyboard
532
Speaker
534
Microphone
536
538
Micro-processor
Short-Range Communications
540
Other Device Subsystems
542
Display
522
Non-volatile Memory
524
RAM
526
Voice Communication Module
Data Communication Module
Other Software Modules
524A
524B
524N
520
DSP
Signals
Control
Rx
512
LOs
513
Signals
Control
Tx
514
511
516
518
500
519

Fig. 2

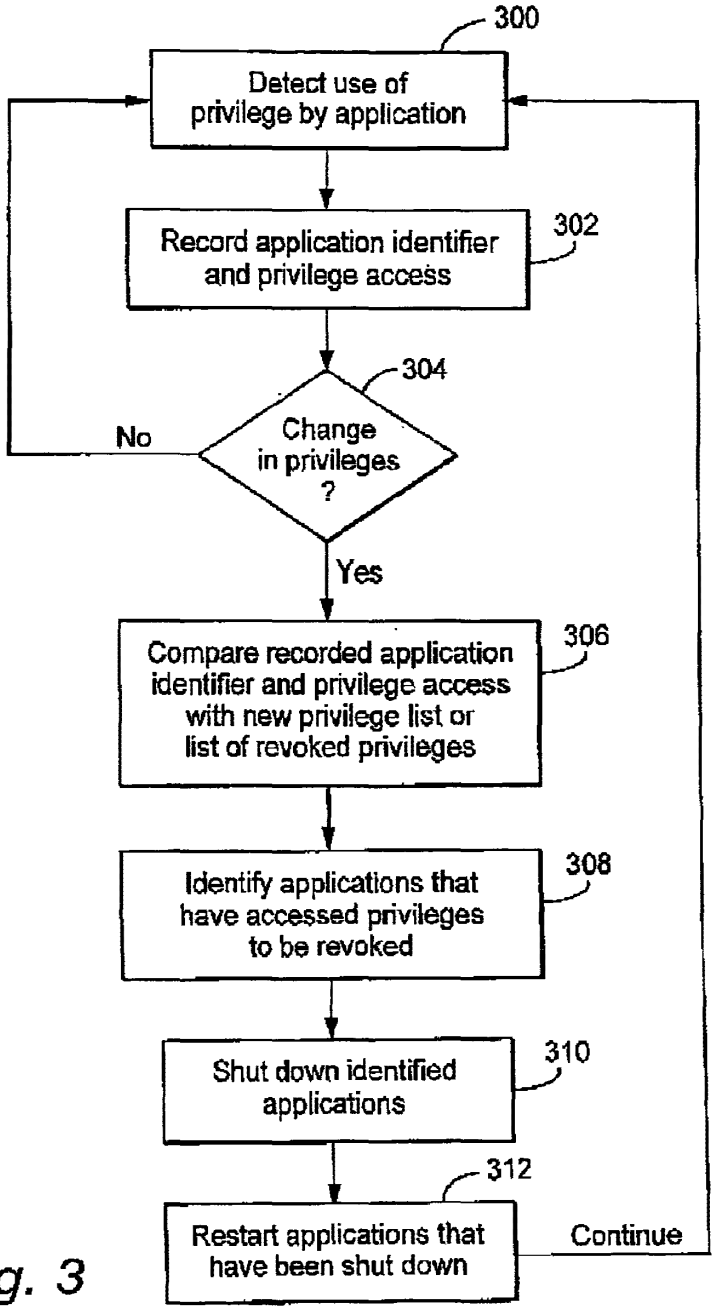

300
Detect use of privilege by application
Record application identifier and privilege access
302
304
Change in privileges ?
No
Yes
Compare recorded application identifier and privilege access with new privilege list or list of revoked privileges
306
Identify applications that have accessed privileges to be revoked
308
Shut down identified applications
310
312
Restart applications that have been shut down
Continue

Fig. 3

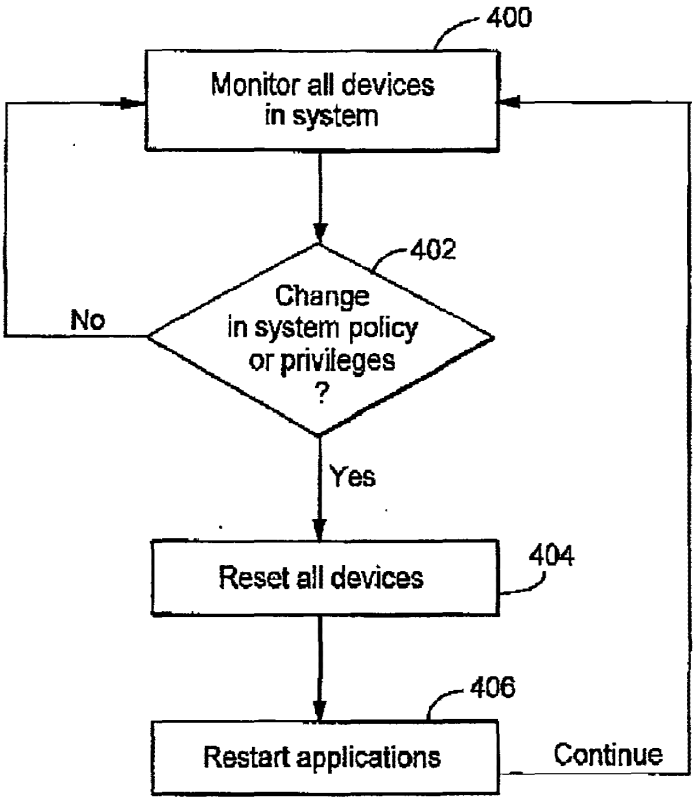

400
Monitor all devices in system
402
Change in system policy or privileges ?
No
Yes
Reset all devices
404
406
Restart applications
Continue

Fig. 4

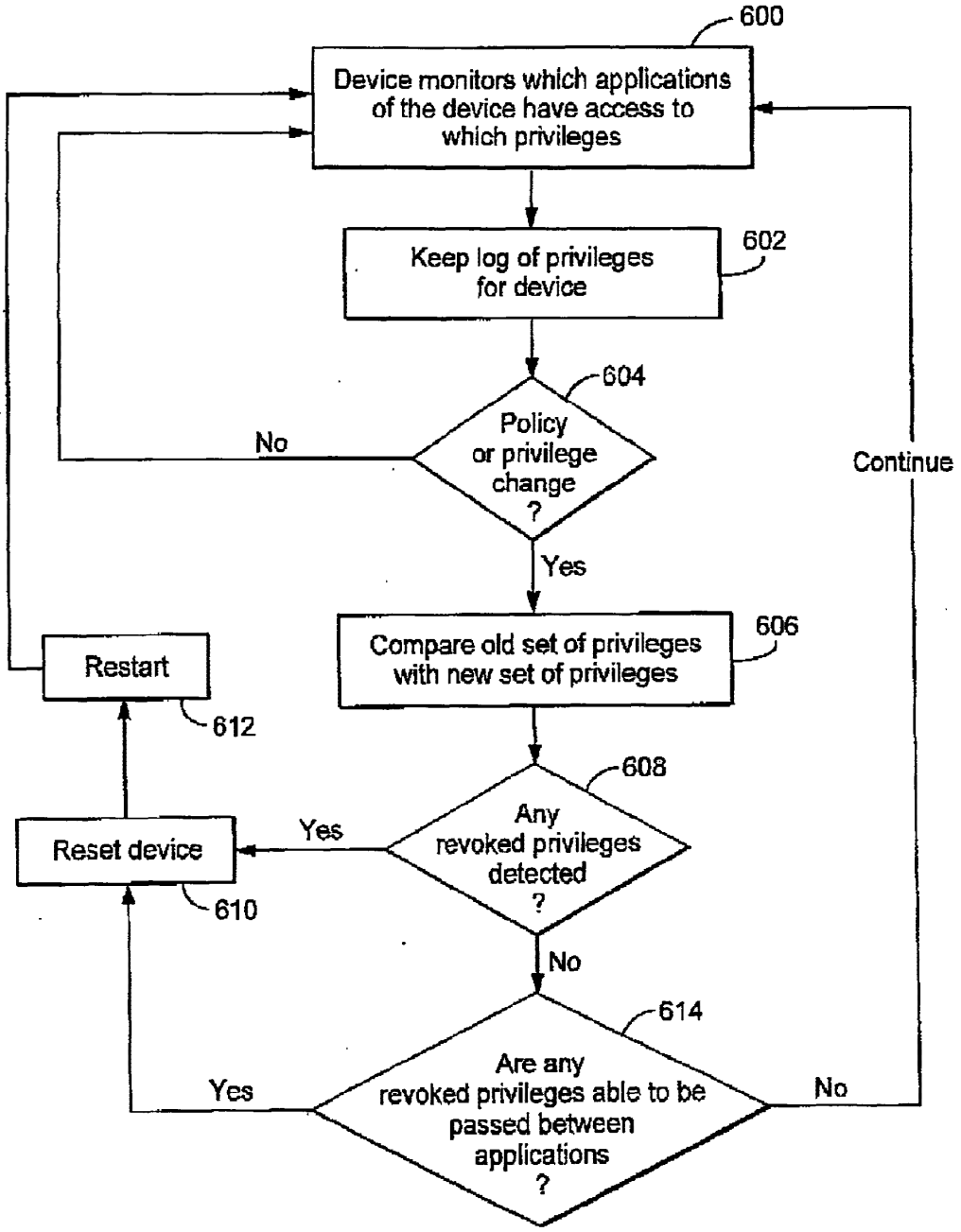

600
Device monitors which applications of the device have access to which privileges
Keep log of privileges for device
602
604
Policy or privilege change ?
No
Yes
Continue
Compare old set of privileges with new set of privileges
606
Restart
612
608
Any revoked privileges detected ?
Yes
Reset device
610
No
614
Are any revoked privileges able to be passed between applications ?
Yes
No

Fig. 5

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 05 25 4068

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	"Using software restriction policies in Windows XP and Windows .NET server to protect against unauthorized software" MICROSOFT WINDOWS XP AND WINDOES .NET TECHNICAL ARTICLE, January 2002 (2002-01), pages 1-52, XP002959638 * abstract * * page 1 * * page 4 * * pages 39-40, chapter "gpupdate.exe" *	9-15	G06F1/00
X	HANS HEDBOM, STEFAN LINDSKOG, STEFAN AXELSSON, ERLAND JONSSON: "Analysis of the Security of Windows NT" ANALYSIS OF THE SECURITY OF WINDOWS NT, 1 March 1999 (1999-03-01), XP002364916 Chalmers University of Technology, Göteborg, SWEDEN * abstract * * page 34, paragraph 5 - page 35, paragraph 5.2 *	9-15	
A	EP 1 043 648 A (SUN MICROSYSTEMS, INC) 11 October 2000 (2000-10-11) * abstract * * page 3, paragraph 10 * * page 4, paragraph 13 - paragraph 14 * * page 5, paragraph 26 * * page 6, paragraphs 35,41 * * page 8, paragraph 49 * * page 9, paragraph 58 - paragraph 64 * * page 11, paragraph 85 - page 12, paragraph 88 *	1-22	TECHNICAL FIELDS SEARCHED (IPC) G06F H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	27 January 2006	Bichler, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 05 25 4068

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-01-2006

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1043648 A	11-10-2000	US 6615264 B1	02-09-2003

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6219694 B **[0018]**

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2007 (21.06.2007)

PCT

(10) International Publication Number
WO 2007/069245 A2

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/IL2006/001428

(22) International Filing Date:
12 December 2006 (12.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/750,326 13 December 2005 (13.12.2005) US
11/376,919 15 March 2006 (15.03.2006) US

(71) Applicant (*for all designated States except US*): **YOGGIE SECURITY SYSTEMS LTD.** [IL/IL]; 42870 Beit Halevy (IL).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): **TOUBOUL, Shlomo** [IL/IL]; Main 6, 42945 Kefar Haim (IL).

(74) Agents: **SANFORD T. COLB & CO.** et al.; P.O. Box 2273, 76122 Rehovot (IL).

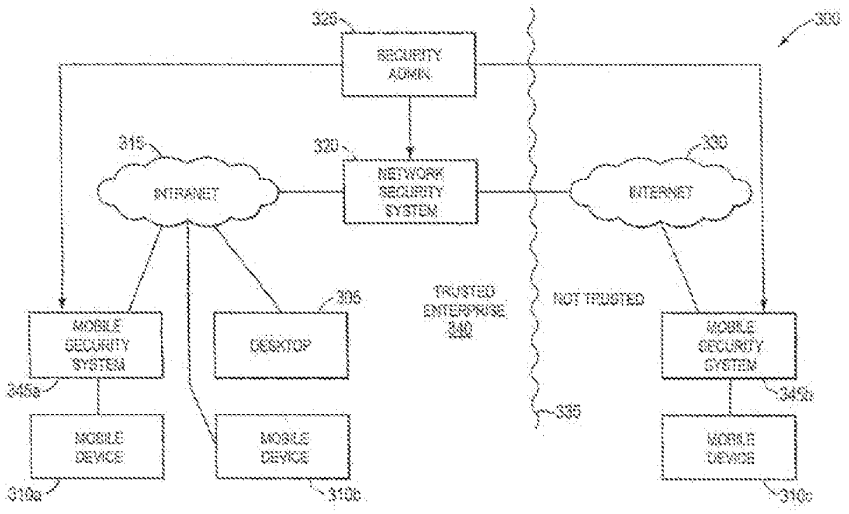
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR,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

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

Published:
— *without international search report and to be republished upon receipt of that report*

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

(54) Title: SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO MOBILE DEVICES



(57) Abstract: A small piece of hardware connects to a mobile device and filters out attacks and malicious code. Using the piece of hardware, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise. In one embodiment, a mobile security system includes a connection mechanism for connecting to a data port of a mobile device and for communicating with the mobile device; a network connection module for acting as a gateway to a network; a security policy for determining whether to forward content intended for the mobile device to the mobile device; and a security engine for executing the security policy.

WO 2007/069245 A2

SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO MOBILE DEVICES

PRIORITY CLAIM

This application claims benefit of and hereby incorporates by reference provisional patent application serial number 60/750,326, entitled "Personal Security Appliance," filed on December 13, 2005, by inventor Shlomo Touboul.

TECHNICAL FIELD

This invention relates generally to network security, and more particularly provides a system and method for providing network security to mobile devices.

BACKGROUND

The internet is an interconnection of millions of individual computer networks owned by governments, universities, nonprofit groups, companies and individuals. While the internet is a great source of valuable information and entertainment, the internet has also become a major source of system damaging and system fatal application code, such as "viruses," "spyware," "adware," "worms," "Trojan horses," and other malicious code.

To protect users, programmers design computer and computer-network security systems for blocking malicious code from attacking both individual and network computers. On the most part, network security systems have been relatively successful. A computer that connects to the internet from within an enterprise's network typically has two lines of defense. The first line of defense includes a network security system, which may be part of the network gateway, that includes firewalls, anti-virus, anti-spyware and content filtering. The second line of defense includes individual security software on individual machines, which is not typically as secure as the network security system and is thus more vulnerable to attacks. In combination, the first and second lines of defense together provide pretty good security protection. However, when a device connects to the internet without the intervening network security system, the device loses its first line of defense. Thus, mobile devices (e.g., laptops, desktops, PDAs such as RIM's Blackberry, cell phones, any wireless device that connects to the internet, etc.) when traveling outside the enterprise network are more vulnerable to attacks.

Figure 1 illustrates an example network system 100 of the prior art. Network system 100 includes a desktop 105 and a mobile device 110, each coupled to an enterprise's intranet 115. The intranet 115 is coupled via a network security system 120 (which may be a part of the enterprise's gateway) to the untrusted internet 130. Accordingly, the desktop 105 and mobile device 110 access the internet 130 via the network security system 120. A security administrator 125 typically manages the network security system 120 to assure that it includes the most current security protection and thus that the desktop 105 and mobile device 110 are protected from malicious code. Demarcation 135 divides the trusted enterprise 140 and the untrusted public internet 130. Because the desktop 105 and the mobile device 110 are connected to the internet

130 via the network security system 120, both have two lines of defense (namely, the network security system 120 and the security software resident on the device itself) against malicious code from the internet 130. Of course, although trusted, the intranet 115 can also be a source of malicious code.

Figure 2 illustrates an example network system 200 of the prior art, when the mobile device 110 has traveled outside the trusted enterprise 140 and reconnected to the untrusted internet 130. This could occur perhaps when the user takes mobile device 110 on travel and connects to the internet 130 at a cybercafé, at a hotel, or via any untrusted wired or wireless connection. Accordingly, as shown, the mobile device 110 is no longer protected by the first line of defense (by the network security system 120) and thus has increased its risk of receiving malicious code. Further, by physically bringing the mobile device 110 back into the trusted enterprise 140 and reconnecting from within, the mobile device 110 risks transferring any malicious code received to the intranet 115.

As the number of mobile devices and the number of attacks grow, mobile security is becoming increasingly important. The problem was emphasized in the recent Info-Security Conference in New York on December 7-8, 2005. However, no complete solutions were presented.

There is a need for personal security appliances capable of providing levels of network security as provided by enterprise network security systems.

SUMMARY

An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

In an embodiment, a mobile security system includes a connection mechanism for connecting to a data port of a mobile device and for communicating with the mobile device; a network connection module for acting as a gateway to a network; a security policy for determining whether to forward content intended for the mobile device to the mobile device; and a security engine for executing the security policy.

The connection mechanism may include at least one of a USB connector, a PCMCIA connector, an Ethernet connector, and a BlueTooth communication module. The network connection module may include a network interface card that implements WiFi, WiMAX, GPRS, GSM, UMTS, CDMA, Generation 3, other cell phone internet connection protocols, etc. The security engine may include at least one of an antivirus engine, an antispyware engine, a firewall engine, an IPS/IDS engine, a content filtering engine, a multilayered security monitor, a bytecode monitor, and a URL monitor. The security policy may performs weighted risk analysis based on content type, content source, content category, or historical actions of the user. The remote management module may be capable of receiving security policy updates, security engine updates, and security data updates (including malicious content signatures). The mobile security system may include a distribution module capable of forwarding updates to other mobile security systems, and/or a backup module capable of storing at least a portion of the boot sector of the mobile device should the boot sector of the mobile device become compromised. The mobile security system may include a remote configuration module capable of communicating with a wizard, the wizard being in communication with an enterprise network security system, the wizard capable of substantially automatic generation of policies and data based on the policies and data on the enterprise network security system, the remote configuration module capable of

installing the policies and data generated by the wizard. The mobile security system may include a preboot memory that is not accessible during runtime, the preboot memory storing a copy of at least a portion of the operating system of the mobile security system, the mobile security system being configured to load the operating system portion every time the mobile security system is rebooted.

In another embodiment, a method comprises receiving a network connection request from a mobile device outside of a trusted network; acting as a gateway to a network on behalf of the mobile device; receiving information intended for the mobile device from the network; and determining whether to forward the information to the mobile device in accordance with a security policy.

In another embodiment, a mobile security system comprises means for acting as a gateway to a network on behalf of a mobile device outside of a trusted network; receiving information intended for the mobile device from the network; and determining whether to forward the information to the mobile device in accordance with a security policy.

In yet another embodiment, a method comprises receiving internet traffic on a mobile device via a wireless connection; redirecting the internet traffic at the kernel level to a mobile security system; scanning the internet traffic for violations of a security policy; cleaning the internet traffic of any violations of the security policy to generate cleaned internet traffic; and sending the cleaned internet traffic to the mobile device for execution.

In still another embodiment, a system comprises a wireless network interface card on a mobile device for receiving internet traffic; a kernel-level redirector on the mobile device for redirecting the internet traffic at the kernel level to a mobile security system; a security engine for scanning the internet traffic for violations of a security policy and for cleaning the internet traffic of any violations of the security policy to generate cleaned internet traffic; and a connection mechanism for receiving the redirected internet traffic from the kernel-level redirector and for sending the cleaned internet traffic to the mobile device for execution.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a prior art network system in a first state.

Figure 2 is a block diagram of a prior art network system in a second state.

Figure 3 is a block diagram of a network system in accordance with an embodiment of the present invention.

Figure 4 is a block diagram illustrating details of a computer system in accordance with an embodiment of the present invention.

Figure 5 is a block diagram illustrating details of the mobile security system in accordance with an embodiment of the present invention.

Figure 6 is a block diagram illustrating details of the mobile security system in accordance with a Microsoft Window's embodiment.

Figures 7 is a block diagram illustrating details of a smart policy updating system in accordance with an embodiment of the present invention.

Figure 8 is a block diagram illustrating details of network security measures relative to the OSI layers.

Figure 9 is a block diagram illustrating details of the communication technique for spreading security code to the mobile security systems.

Figures 10A-10C are block diagrams illustrating various architectures for connecting a mobile device to a mobile security system, in accordance with various embodiments of the present invention.

DETAILED DESCRIPTION

The following description is provided to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the embodiments may be possible to those skilled in the art, and the generic principles defined herein may be applied to these and other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein.

An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

Figure 3 illustrates a network system 300 in accordance with an embodiment of the present invention. Network system 300 includes a desktop 305, a first mobile device 310a, and a second mobile device 310b. The first mobile device 310a is illustrated as within the enterprise network 340 at this time and is coupled via a mobile security system 345a to the enterprise's intranet 315. The desktop 305 and second mobile device 310b are also within the enterprise network 340 but in this embodiment are coupled to the intranet 315 without an intervening mobile security system 345 such as mobile security system 345b. The intranet 315 is coupled via a network security system 320 (which may be part of the enterprise's gateway) to the untrusted internet 330. Accordingly, the first mobile device 310a, the second mobile device 310b and the desktop 305 access the untrusted internet 330 via the network security system 320. Each may also be protected by a personal security system resident thereon (not shown). A third mobile device 310c is currently outside the enterprise network 340 and is coupled via a mobile security system 345b to the untrusted internet 330. The third mobile device 310 may be in use by an employee of the trusted enterprise 340 who is currently on travel. A security administrator 325 manages the mobile security system 345a, the mobile security system 345b, and the network

security system 320 to assure that they include the most current security protection. One skilled in the art will recognize that the same security administrator need not manage the various devices. Further, the security administrator could be the user and need not be within the trusted enterprise 340.

Demarcation 335 divides the trusted enterprise 340 and the untrusted publicly accessible internet 330. Each of mobile device 310a, 310b and 310c may be referred to generically as mobile device 310, although they need not be identical. Each mobile security system 345a and 345b may be referred to generically as mobile security system 345, although they need not be identical.

As shown, although the mobile device 310c has traveled outside the trusted enterprise 340, the mobile device 310c connects to the untrusted internet 330 via the mobile security system 345b and thus retains two lines of defense (namely, the mobile security system 345b and the security software resident on the device itself). In this embodiment, the mobile security system 345 effectively acts as a mobile internet gateway on behalf of the mobile device 310c. In an embodiment, the mobile security system 345 may be a device dedicated to network security. In an embodiment, each mobile security system 345 may support multiple mobile devices 310, and possibly only registered mobile devices 310, e.g., those belonging to enterprise 340.

Each mobile security system 345 (e.g., 345a, 345b) may be a miniature server, based on commercial hardware (with Intel's Xscale as the core), Linux OS and network services, and open-source firewall, IDS/IPS and antivirus protection. The mobile security system 345 may be based on a hardened embedded Linux 2.6.

In this embodiment, because the security administrator 325 is capable of remotely communicating with the mobile security system 345b, IT can monitor and/or update the security policies/data/engines implemented on the mobile security system 345b. The security administrator 325 can centrally manage all enterprise devices, remotely or directly. Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security

systems 345 accordingly. Because the mobile security system 345 may be generated from the relevant security policies of the enterprise 340, the mobile device 310c currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise 340.

The mobile security system 345 may be designed as an add-on to existing software security or to replace all security hardware and software on a traveling mobile device. These security applications will preferably operate on different OSI layers to provide maximum security and malicious code detection, as shown in the example system illustrated in Figure 8. Operating on the lower OSI layers and doing TCP/IP packets analysis only (by screening firewall or router packets) would miss virus and/or worm behavior. Also, many modern viruses use mobile code implemented on a "higher" level than the 7th OSI layer (Application – HTTP, FTP, etc.) and therefore cannot be interpreted at the packet layer nor at the application layer. For example, applying antivirus analysis only at the session or transport layer on a malicious Java Script (that is included in an HTML page), trying to match the signature with packets and without understanding the content type (Java Script), will not detect the malicious nature of the Java Script. To offer greater protection, the mobile security system 345 may act as corporate class security appliance and engage different security applications based on the content type and the appropriate OSI layers, (or even a "higher" level if content is encapsulated in the application layer). The mobile security system 345 may be configured to perform content analysis at different OSI layers, e.g., from the packet level to the application level. It will be appreciated that performing deep inspection at the application level is critical to detect malicious content behavior and improve detection of viruses, worms, spyware, Trojan horses, etc. The following software packages may be implemented on the mobile security system 345:

- Firewall and VPN – including stateful and stateless firewalls, NAT, packet filtering and manipulation, DOS/DDOS, netfilter, isolate user mobile devices from the internet and run VPN program on the device, etc.
- Optional web accelerator and bandwidth/cache management based on Squid.
- IDS/IPS – Intrusion detection and prevention system based on Snort. Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol- and anomaly-based inspections.

- Antivirus and antispyware based on ClamAV; additional AV and AS engines, e.g., McAfee, Kaspersky, Pandamay, may be offered for additional subscription fees.
- Malicious Content Detection – on the fly heuristics that perform content analysis to detect malicious content before having signatures. This will be based on a rule base and updated rules and will be content dependent scanning.
- URL Categorization Filtering – based on a commercial engine, such as Surfcontrol, Smart Filters or Websense. May provide around 70 categories of URLs such as gambling, adult content, news, webmail, etc. The mobile device 345 may apply different security policies based on the URL category, e.g., higher restriction and heuristics for Gambling or Adult content web sites, etc.

FIG. 4 is a block diagram illustrating details of an example computer system 400, of which each desktop 305, mobile device 310, network security system 320, mobile security system 345, and security administrator 325 may be an instance. Computer system 400 includes a processor 405, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 410. The computer system 400 further includes an input device 415 such as a keyboard or mouse, an output device 420 such as a cathode ray tube display, a communications device 425, a data storage device 430 such as a magnetic disk, and memory 435 such as Random-Access Memory (RAM), each coupled to the communications channel 410. The communications interface 425 may be coupled directly or via a mobile security system 345 to a network such as the internet. One skilled in the art will recognize that, although the data storage device 430 and memory 435 are illustrated as different units, the data storage device 430 and memory 435 can be parts of the same unit, distributed units, virtual memory, etc.

The data storage device 430 and/or memory 435 may store an operating system 440 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, UNIX OS, LINUX OS and/or other programs 445. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology.

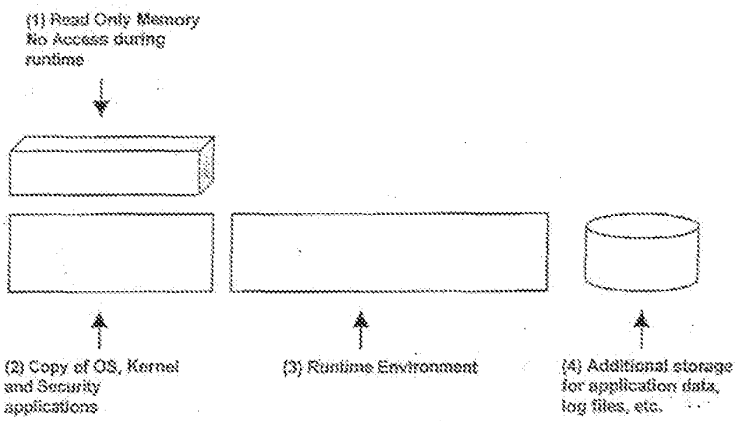
One skilled in the art will recognize that the computer system 400 may also include additional information, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc. One skilled in the art will also recognize that the programs and data may be received by and stored in the system in alternative ways. For example, a computer-readable storage medium (CRSM) reader 450 such as a magnetic disk drive, hard disk drive, magneto-optical reader, CPU, etc. may be coupled to the communications bus 410 for reading a computer-readable storage medium (CRSM) 455 such as a magnetic disk, a hard disk, a magneto-optical disk, RAM, etc. Accordingly, the computer system 400 may receive programs and/or data via the CRSM reader 450. Further, it will be appreciated that the term "memory" herein is intended to cover all data storage media whether permanent or temporary.

Figure 5 is a block diagram illustrating details of the mobile security system 345 in accordance with an embodiment of the present invention. Mobile security system 345 includes adapters/ports/drivers 505, memory 510, a processor 515, a preboot flash/ROM memory module 520 storing a secure version of the mobile security system's operating system and other applications, network connection module 525, security engines 530, security policies 535, security data 540, remote management module 550, distribution module 555, and backup module 560. Although these modules are illustrated as within the mobile security system 345, one skilled in the art will recognize that many of them could be located elsewhere, e.g., on the security administrator 325 or on third-party systems in communication with the mobile security system 345. The mobile security system 345 may be in a pocket-size, handheld-size or key-chain size housing, or possibly smaller. Further, the mobile security system 345 may be incorporated within the mobile device 310.

The adapters/ports/drivers 505 include connection mechanisms (including software, e.g., drivers) for USB, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection data ports on the mobile security system 345. In one embodiment, the adapters/ports/drivers 505 may be capable of connection to multiple devices 310 to provide network security to the multiple devices 310.

Memory 510 and processor 515 execute the operating system and applications on the mobile security system 345. In this example, the preboot flash 520 stores the operating system and applications. At boot time, the operating system and applications are loaded from the preboot flash 520 into memory 510 for execution. Since the operating system and applications are stored in the preboot flash 520, which cannot be accessed during runtime by the user, the operating system and applications in the preboot flash 520 are not corruptible. Should the copy of the operating system and applications in memory 510 be corrupted, e.g., by malicious code, the operating system and applications may be reloaded into the memory 510 from the preboot flash 520, e.g., upon restart. Although described as stored within the preboot flash 520, the OS and applications can be securely stored within other read-only memory devices, such as ROM, PROM, EEPROM, etc.

Memory (including memory 510 and preboot flash 520) on the mobile security system 345 may be divided into zones as follows:



Upon each "hard" restart, the boot loader (resident at area 1) of the mobile security system 345 copies the kernel and security applications (a fresh unchanged copy) from area 1 to 2. This causes a clean version of the OS and applications to be loaded into area 2 each time. That way, if a special mobile security system 345 attack is developed, the attack will be unable to infect the

system, since the OS and applications are precluded from accessing memory area 1 during runtime. Further, any attack that does reach memory 510 will be able to run only once and will disappear upon a hard restart. A triggering mechanism may be available to restart the mobile security system 345 automatically upon infection detection.

The network connection module 525 enables network connection, e.g., to the internet 330 or the intranet 315 via network communication hardware/software including WiFi, WiMAX, CDMA, GSM, GPRS, Ethernet, modem, etc. For example, if the mobile device 310 wishes to connect to the internet 330 via a WiFi connection, the adapters/ports/drivers 505 may be connected to the PCI port, USB port or PCMCIA port of the mobile device 310, and the network connection module 525 of the mobile security system 345 may include a WiFi network interface card for connecting to wireless access points. Using the network connection module 425, the mobile security system 345 may communicate with the network as a secure gateway for the mobile device 310. Other connection architectures are described in Figures 10A-10C.

The security engines 530 execute security programs based on the security policies 535 and on security data 540, both of which may be developed by IT managers. Security engines 530 may include firewalls, VPN, IPS/IDS, anti-virus, anti-spyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. Each security engine 530 may have dedicated security policies 535 and security data 540 to indicate which procedures, content, URLs, system calls, etc. the engines 530 may or may not allow. The security engines 530, security policies 535 and security data 540 may be the same as, a subset of, and/or developed from the engines, policies and data on the network security system 320.

To provide a higher security level provided by antivirus and antispyware software, the security engines 530 on each mobile security system 345 may implement content analysis and risk assessment algorithms. Operating for example at OSI Layer 7 and above (mobile code encapsulated within Layer 7), these algorithms may be executed by dedicated High Risk Content Filtering (HRCF) that can be controlled by a rules engine and rule updates. The HRCF will be based on a powerful detection library that can perform deep content analysis to verify real content types. This is because many attacks are hidden within wrong mime types and/or may use

sophisticated tricks to present a text file type to a dangerous active script or ActiveX content type. The HRCF may integrate with a URL categorization security engine 530 for automatic rule adjustment based on the URL category. In one embodiment, when the risk level increases (using the described mechanism) the mobile security system 345 may automatically adjust and increase filtering to remove more active content from the traffic. For example, if greater risk is determined, every piece of mobile code, e.g., Java script, VB script, etc. may be stripped out.

Three aspects for integration with corporate policy server legacy systems include rules, LDAP and active directory, and logging and reporting as discussed below. In one embodiment, a policy import agent running on the security administrator 325 will access the rule base of Checkpoint Firewall-1 and Cisco PIX Firewalls and import them into a local copy. A rule analysis module will process the important rules and will offer out-of-the-box rules and policies for mobile security systems 345. This proposed policy will offer all mobile security systems 345 a best fit of rules that conform the firewall policy of the enterprise 340. The agent will run periodically to reflect any changes and generate updates for mobile security system 345 policies 535. The LDAP and Active Directory may be integrated with the directory service to maintain mobile security system 345 security policies 535 that respond to the enterprise's directory definitions. For example, a corporate policy for LDAP user Group "G" may automatically propagate to all mobile security systems 345 in "G" group. Mobile security system 345 local logs and audit trails may be sent in accordance to a logging and reporting policy to a central log stored at the security administrator 325. Using a web interface, IT may be able to generate reports and audit views related to all mobile device 310 users, their internet experiences, and attempts to bring infected devices back to the enterprise 340. IT will be able to forward events and log records into legacy management systems via SYSLOG and SNMP Traps.

The security engines 530 may perform weighted risk analysis. For example, the security engine 530 may analyze HTTP, FTP, SMTP, POP3, IM, P2P, etc. including any traffic arriving from the internet 330. The security engine 530 may assign a weight and rank for every object based on its type, complexity, richness in abilities, source of the object, etc. The security engine 530 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 530 may assign weight to objects based on the category of the

source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 530 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 530 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

In some embodiments, the security engines 530, security policies 535 and security data 540 may enable bypassing the mobile security system 345. The security policy 535, set by the security administrator 325, may include a special attribute to force network connection through the mobile security system 325 when outside the trusted enterprise 340. Thus, if this attribute is set "on," when a mobile device 310 attempts to connect to the internet 330 without the mobile security system 345 and not from within the trusted enterprise 340, all data transfer connections including LAN connection, USB-net, modem, Bluetooth, WiFi, etc. may be closed. The mobile device 310 may be totally isolated and unable to connect to any network, including the internet 330.

In one embodiment, to enable this, when first connecting the mobile security system 345 to the mobile device 310 using for example the USB cable (for both power and USB connection creation), the USB plug & play device driver will be sent into the mobile device 310. The installed driver may be "Linux.inf" which allows a USB-net connection for the mobile security system 345. This connection allows the mobile security system 345 to access the internet 330 via the USB port and using the mobile device 310 network connection plus additional code ("the connection client"). In a Windows example, the connection client may be installed at the NDIS level of the mobile device 310 above all the network interface cards of every network connection as shown in Figure 6. The implementation will be as an NDIS Intermediate (IM) Driver or NDIS-Hooking Filter Driver. Both implementations may be at the kernel level, so that an end user cannot stop or remove it. When starting the mobile device 310, the connection client may attempt to connect to the security administrator 325 or the network security system 320 locally

within the trusted enterprise 340. If the node is not found (finding via VPN is considered as not found in local LAN), the connection client will assume it is working from outside the trusted enterprise 340 and expects to find the mobile security system 345 connected, e.g., via USB-net or other connection mechanism. If the mobile security system 345 is not found, the connection client may avoid any communication to any network connection. By a policy definition, this behavior can be modified to allow communication to the enterprise 340 via VPN installed in the mobile device 310. Similarly, in case of a mobile device system 345 failure, all traffic may be disabled, except for the VPN connection into the enterprise 340.

It will be appreciated that NDIS is one possible implementation of intercepting traffic at the kernel level. For example, in another embodiment, the system may hook Winsock or apply other ways that may be in future Windows versions.

In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (e.g., based on for example user preferences or IT decision). Alternatively, it can apply the same engines 530, policies 535 and data 540 for all connected devices 310.

The remote management module 550 enables communication with security administrator 325 (and/or other security administrators), and enables local updating of security engines 530, security policies 535, security data 540 including signatures and other applications. In one embodiment, modification to the security policies 535 and data 540 can be done by the security administrator 325 only. The remote management module 550 of the mobile security system 345 may receive updates from an update authorities device (UAD), e.g., on the security administrator 325 via a secured connection. A UAD may operate on an update server at a customer IT center located on the internet 330 to forward updates to mobile security systems 345 that possibly do not belong to an enterprise 540 in charge of managing updates. A UAD may operate on a mobile security system 345. Security engine 530 updates may modify the antivirus engine DLL, etc. OS and security application updates may be implemented only from within the enterprise 540

while connecting to the security administrator 325 and via an encrypted and authenticated connection.

The security administrator 325 can modify URL black and white lists for remote support to traveling users. In case of false positives, the security administrator 325 may allow access to certain URLs, by bypassing the proactive heuristics security but still monitoring by firewall, antivirus, IPS/IDS, etc. Additional remote device-management features may enable the security administrator 325 to perform remote diagnostics, access local logs, change configuration parameters, etc. on the mobile security system 345. The security administrator 325 may delegate tasks to a helpdesk for support.

The remote management module 550 may communicate with a wizard (e.g., wizard 745), which may be on the security administrator 325, as illustrated in Figure 7, or on another system. Details of the wizard 745 and details of the communication schemes between the remote management module 550 and the wizard 745 are described below with reference to Figure 7.

The distribution module 555 enables distribution of updates, e.g., security policy 535 updates including rule updates, security data 540 updates including signature updates, security engine 530 updates, application/OS updates, etc. by the mobile security system 345 to N other mobile security systems 345. A routing table identifying the N other mobile security systems 345 to whom to forward the updates may be provided to the distribution module 555 to enable system 345 to system 345 communication. Updates may be implemented according to policies set by the security administrator 325. When forwarding updates, the distribution module 555 acts as a UAD.

Each mobile security system 345 may obtain its routing table with security information updates, periodically, at predetermined times, upon login, etc. The routing tables may be maintained on a server, e.g., the security administrator 325 or another mobile security system 345. In one embodiment, the mobile security systems 345 may contact the server to retrieve the routing tables. Alternatively, the server may push the routing tables to the mobile security systems 345.

The distribution module 555 may enable rapid updates as shown in Figure 9. Currently, all commercial antivirus products available do not update devices faster than viruses spread. To assure that a new virus attack does not spread faster than for example signature updates, each mobile security system 345 may be an active UAD. In one embodiment, as shown in Figure 9, each mobile security system 345 is responsible for forwarding the signature updates to four other devices 345. As one skilled in the art will recognize, all devices 345 need to forward to the same number of other devices 345. Multiple devices 345 may be responsible for forwarding to the same device 345. When necessary, offline devices 345 being activated may poll the server, e.g., the security administrator 325, for routing table updates. Many other updating techniques are also possible.

The backup module 560 may constantly backup image and changes of the boot sector and system files of the mobile device 310 into the flash memory 520 or into another persistent memory device. That way, in case of major failure, including a loss of the system or boot sector of the mobile device 310, the mobile security system 345 may be identified as a CD-ROM during reboot and may launch the backup module (or separate program) to restore the boot sector and system files on the mobile device 310, thereby recovering the mobile device 310 without the need for IT support. In an embodiment where the network security system 345 supports multiple mobile devices 310, the backup module 560 may contain separate boot sector and system files for each of the mobile devices 310, if different.

Figure 7 is a block diagram illustrating details of a smart policy updating system 700 in accordance with an embodiment of the present invention. System 700 includes the security administrator 325 coupled to the network security system 320 and to the mobile security system 345. The network security system 320 includes security engines 705, including an antivirus engine 715, an IPS/IDS engine 720, a firewall engine 725, and other security engines. The network security system 320 also includes security policies and data 710, including antivirus policies and data 730, IPS/IDS policies and data 735, firewall policies and data 740, and other policies and data. Similarly, the mobile security system 345 includes an antivirus engine 755, an IPS/IDS engine 760, a firewall engine 765, and other engines. The mobile security system 345

also includes security policies and data 535/540, including antivirus security policies and data 770, IPS/IDS security policies and data 775, firewall security policies and data 780, and other security policies and data.

The security administrator 325 includes a wizard 745 for enabling substantially automatic initial and possibly dynamic setup of the security engines 530, security policies 535 and security data 540 on the mobile security system 345. In one embodiment, the wizard 745 may automatically load all security engines 705 and policies and data 710 of the network security system 320 as the security engines 530 and policies and data 535/540 on the mobile security system 345. In another embodiment, the wizard 745 may include all security engines 705 and policies and data 710 except those known to be irrelevant, e.g., those related to billing software used by accounting, those relating to web software running only on the web servers, etc. In another embodiment, the engines 530 would need to be loaded by an IT manager, and would not be loaded automatically by the wizard 745.

In one embodiment, the wizard 745 may determine whether the mobile security system 345 requires a particular security engine 530, e.g., an antivirus engine 755, IPS/IDS engine 760, firewall engine 765, etc. If so determined, then the wizard 745 would load the engine 530 onto the mobile security system 345. The wizard 745 would then determine which policies and data sets, e.g., some for antivirus engine 755, some for the IPS/IDS engine 760, some for the firewall engine 765, etc. are important to the mobile security system 345. The wizard 745 will then determine which of the antivirus policies and data 730 on the network security system 320 are relevant to the antivirus policies and data 770 on the mobile security system 345, which of the IPS/IDS policies and data 735 on the network security system 320 are relevant to the IPS/IDS policies and data 775 on the mobile security system 345, which of the firewall policies and data 740 on the network security system 320 are relevant to the firewall policies and data 780 on the mobile security system 345, and which of the other policies and data on the network security system 320 are relevant to the policies and data on the mobile security system 345. As stated above, the wizard 745 may determine that all security engines 705 or just a subset are needed on the mobile security system 345. The wizard 745 may determine that all policies and data 710 for a given engine type or just a subset should be forwarded. The wizard 745 may determine which

relevant policies and data 710 should be forwarded to the mobile security system 345 based on rules developed by an IT manager, based on item-by-item selection during the setup procedure, etc. Alternative to the wizard 745, an IT manager can setup the engines 530 and policies and data 535/540 on the mobile security system 345 without the wizard 745.

The security administrator 325 may also include an update authorities device 750. The update authorities device 750 may obtain security system updates (e.g., signature updates) and may send the updates to the network security system 320 and to the mobile security system 345. One skilled in the art will recognize that the updates to the network security system 320 and the updates to the mobile security system 345 need not be the same. Further, the update authorities device 750 may obtain the updates from security managers, security engine developers, antivirus specialists, etc. The update authorities device 750 may forward the updates to all network security systems 320 and all mobile security systems 345, or may forward routing tables to all mobile security systems 345 and the updates only to an initial set of mobile security systems 345. The initial set of mobile security systems 345 may forward the updates to the mobile security systems 345 identified in the routing tables in a P2P manner, similar to the process illustrated in Figure 9. As stated above, each mobile security system 345 operating to forward updates is itself acting as an update authorities device 750.

Other applications may be included on the mobile security system 345. For example, add-on applications for recurring revenue from existing customers may include general email, anti-spam, direct and secured email delivery, information vaults, safe skype and other instant messaging services, etc.

- Email Security and Anti-spam – implementation of mail relay on mobile security systems 345 (including the web security engine above) and a local spam quarantine (based on SendMail or similar process) may implement a complete mail security suite (SMTP and POP3) including anti-spam with real time indexing (via online web spam quarries). Users may have access to the quarantine to review spam messages, release messages, modify and custom spam rules, etc., via a web interface.
- Direct and Secured Email Delivery based on mail relay will allow the mobile security system 345 to send user email directly from one mobile security system 345 to another

mobile security system 345 without using in route mail servers. This allows corporate users to send emails that need not travel in the internet, thus leaving trace and duplicates on different unknown mail servers in route. This combined with the ability to use a secured pipe between two mobile security systems is valuable to corporations. Without such methodology, people could trace emails exchange without accessing to the enterprise's mail server, by tracking down copies in intermediate mail servers that were used to deliver the messages.

* Information Vault – Application to encrypt and store end user information on the mobile security system 345 may be available only to authorized users via a web interface and a web server implemented on every mobile security system 345 (e.g., BOA, Apache, etc.)
* Safe Skype and Other IM – implementing an instant messaging client on the mobile security system 345 can guarantee that the instant messaging system or P2P application has no access to data on the mobile device 310. Adding a chipset of AC/97 to provide a sound interface on the mobile security system 325 could allow users to talk and receive calls directly from/to the mobile security system 325.

Although not shown, a small battery may be included with the mobile security system 345. This battery may be charged by the USB connection during runtime or using the power adapter at any time. The battery may guarantee proper shutdown, e.g., when user disconnects the USB cable from the mobile security system 345. It will be signaled by the system which will launch applications and system shutdown. This will ensure a proper state of the file system and flashing open files buffers.

A multi-layered defense and detection abilities is required. This may be done by a special code that is constantly monitoring the scanning result by different systems (antivirus, IDS/IPS, firewall, antispyware, URL category, etc.) and at different levels to build a puzzle and identify an attack even if its not recognized by each of the individual subsystems. By doing this, the mobile security system 345 will maintain and in some cases even improve the security level provided within the enterprise 540.

One available benefit of the mobile security system 345 is its ability to enforce the policy of the enterprise 540 on the end user while they are traveling or working from home. Since the mobile security system 345 uses similar security engines and policy as when connected from within the enterprise 540 and since the end user cannot access the internet 330 without it (except via VPN connection into the enterprise 540), IT may be capable of enforcing its security policy beyond the boundaries of the enterprise 540. The OS may be under the entire supervision of IT, while the mobile security system 345 OS acts as an end user OS under his control. This resolves the problems of who controls what and how security and productivity face minimal compromise.

A standalone version of the mobile security system 345 may offer the same functionality, and may provide a local management interface via web browser. Attractive to home users and small offices that lack an IT department, the mobile security system 345 enables the end user to launch a browser, connect to the mobile security system 345, set the different policies (update policy, security rules, etc.) including modifying the white and black URL lists, etc. There is also an opportunity to provide end users with a service of remote management of the mobile security systems 345 by subscription.

Figures 10A, 10B and 10C illustrate three example architectures of connecting a mobile security system 345 to a mobile device 310, in accordance with various embodiments of the present invention. In Figure 10A, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1015 and 1020 and is coupled to the internet 330 via a NIC card 1005. The mobile device 310 receives internet traffic from the internet 330 via its NIC card 1005. A kernel-level redirector 1010 (e.g., via NDIS, Winsock, etc.) on the mobile device 310 automatically redirects the internet traffic via the USB connections 1015 and 1020 to the mobile security system 345, which scans, cleans and returns the cleaned internet traffic to the mobile device 310 via the USB connections 1015 and 1020. In Figure 10B, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1025 and 1030. The mobile security system 345 includes a NIC card 1035 for receiving internet traffic from the internet 330. The mobile security system 345 scans, cleans and forwards the internet traffic via the USB connections 1025 and 1030 to the mobile device 310. In Figure 10C, the mobile device 310 is coupled to the mobile security system 345 via NIC cards 1040 and 1045. The mobile security

system 345 receives internet traffic from the internet 330 via its NIC card 1045. The mobile security system 345 scans, cleans and forwards the internet traffic wirelessly via the NIC cards 1040 and 1045 to the mobile device 310. Other connection architectures are also possible.

The foregoing description of the preferred embodiments of the present invention is by way of example only, and other variations and modifications of the above-described embodiments and methods are possible in light of the foregoing teaching. Although the network sites are being described as separate and distinct sites, one skilled in the art will recognize that these sites may be a part of an integral site, may each include portions of multiple sites, or may include combinations of single and multiple sites. The various embodiments set forth herein may be implemented utilizing hardware, software, or any desired combination thereof. For that matter, any type of logic may be utilized which is capable of implementing the various functionality set forth herein. Components may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. Connections may be wired, wireless, modem, etc. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

CLAIMS

1. A mobile security system, comprising:

a connection mechanism for connecting to a data port of a mobile device and for communicating with the mobile device;

a network connection module for acting as a gateway to a network;

a security policy for determining whether to forward content intended for the mobile device to the mobile device; and

a security engine for executing the security policy.

2. The mobile security system of claim 1, wherein the connection mechanism includes at least one of a USB connector, a PCMCIA connector, an Ethernet connector, and a wireless communication module.

3. The mobile security system of claim 1, wherein the network connection module includes a wireless network interface card.

4. The mobile security system of claim 1, wherein the security engine includes at least one of an antivirus engine, an antispyware engine, a firewall engine, an IPS/IDS engine, a content filtering engine, a multilayered security monitor, a bytecode monitor, and a URL monitor.

5. The mobile security system of claim 1, wherein the security policy performs weighted risk analysis.

6. The mobile security system of claim 5, wherein the weighted risk analysis weighs risk based on content type.

7. The mobile security system of claim 5, wherein the weighted risk analysis weighs risk based on content source.

8. The mobile security system of claim 5, wherein the weighted risk analysis weighs risk based on content source category.

9. The mobile security system of claim 5, wherein the weighted risk analysis weighs risk based on historical actions of the user.

10. The mobile security system of claim 1, further comprising a remote management module capable of receiving security policy updates.

11. The mobile security system of claim 1, further comprising a remote management module capable of receiving security engine updates.

12. The mobile security system of claim 1, further comprising security data and a remote management module capable of receiving security data updates.

13. The mobile security system of claim 1, wherein the security data includes malicious content signatures.

14. The mobile security system of claim 1, further comprising a distribution module capable of forwarding updates to other mobile security systems.

15. The mobile security system of claim 1, further comprising a backup module capable of storing at least a portion of the boot sector of the mobile device should the boot sector of the mobile device become compromised.

16. The mobile security system of claim 1, further comprising a remote configuration module capable of communicating with a wizard, the wizard being in communication with an enterprise network security system, the wizard capable of substantially automatic generation of policies and data based on the policies and data on the enterprise network security system, the remote configuration module capable of installing the policies and data generated by the wizard.

17. The mobile security system of claim 1, further comprising a preboot memory that is not accessible during runtime, the preboot memory storing a copy of at least a portion of the operating system of the mobile security system, the mobile security system being configured to load the operating system portion every time the mobile security system is rebooted.

18. A method comprising:

receiving a network connection request from a mobile device when the mobile device is outside of a trusted network;

acting as a gateway to a network on behalf of the mobile device;

receiving information intended for the mobile device from the network; and

determining whether to forward the information to the mobile device in accordance with a security policy.

19. A system comprising:

means for acting as a gateway to a network on behalf of a mobile device when the mobile device is outside of a trusted network;

receiving information intended for the mobile device from the network; and

determining whether to forward the information to the mobile device in accordance with a security policy.

20. A method comprising:

receiving internet traffic on a mobile device via a wireless connection;

redirecting the internet traffic at the kernel level to a mobile security system;

scanning the internet traffic for violations of a security policy;

cleaning the internet traffic of any violations of the security policy to generate cleaned internet traffic; and

sending the cleaned internet traffic to the mobile device for execution.

21. A system comprising:

a wireless network interface card on a mobile device for receiving internet traffic;

a kernel-level redirector on the mobile device for redirecting the internet traffic at the kernel level to a mobile security system;

a security engine for scanning the internet traffic for violations of a security policy and for cleaning the internet traffic of any violations of the security policy to generate cleaned internet traffic; and

a connection mechanism for receiving the redirected internet traffic from the kernel-level redirector and for sending the cleaned internet traffic to the mobile device for execution.

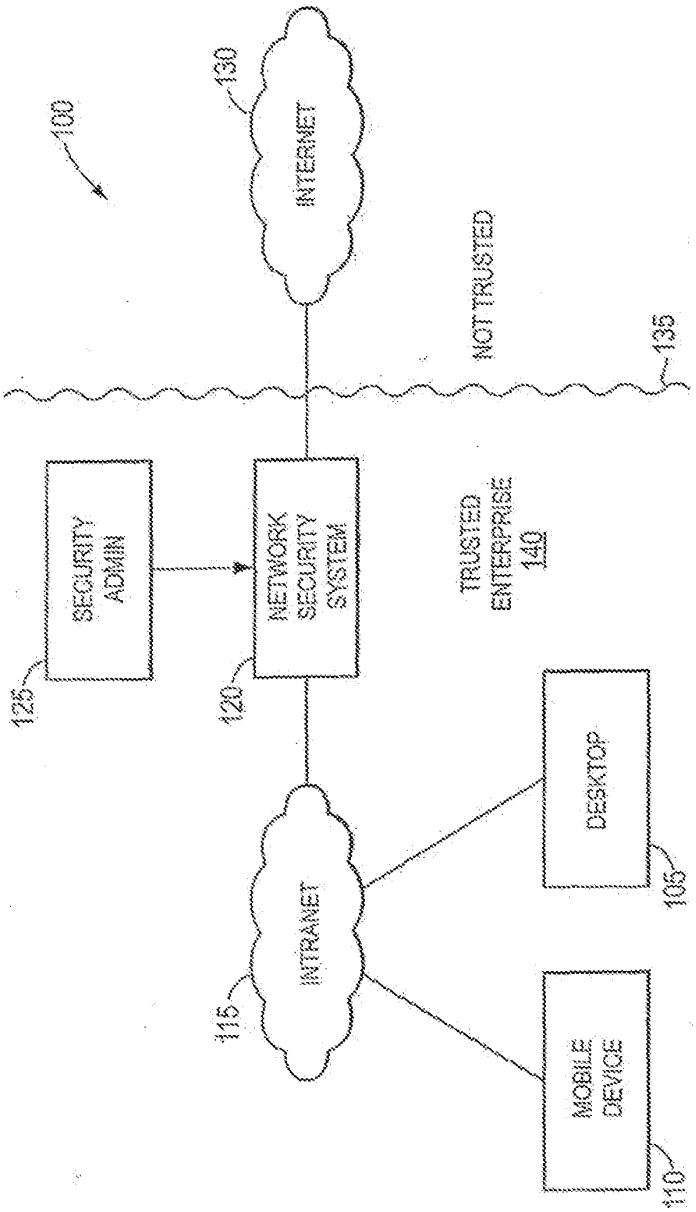


FIG. 1
(PRIOR ART)

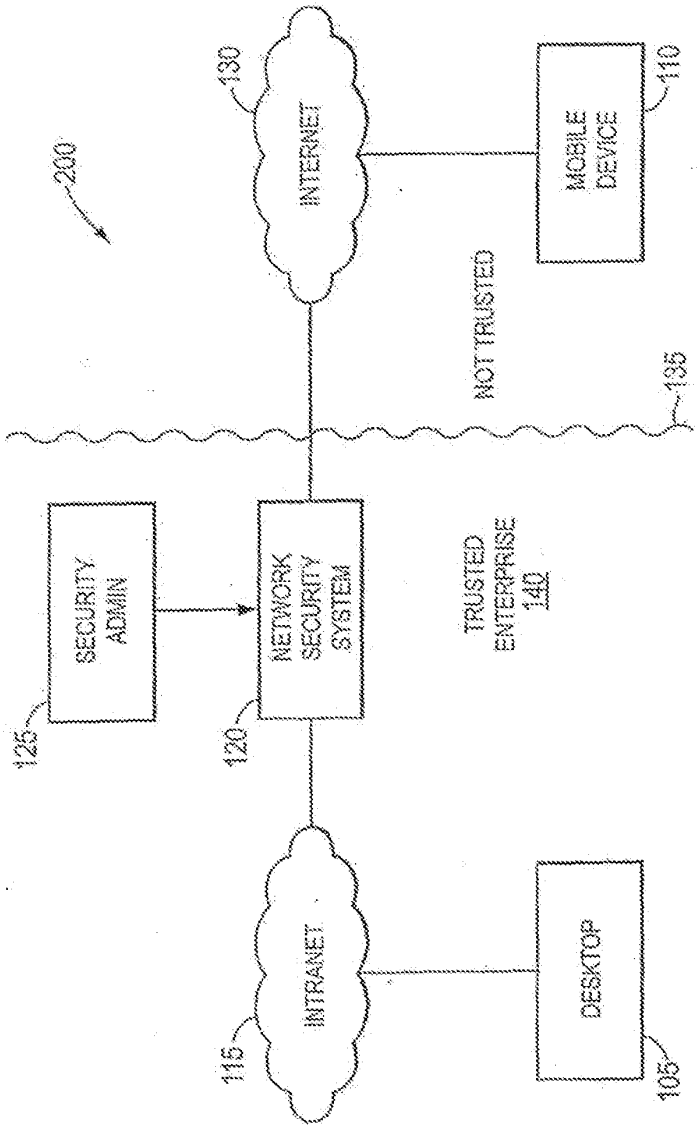


FIG. 2
(PRIOR ART)

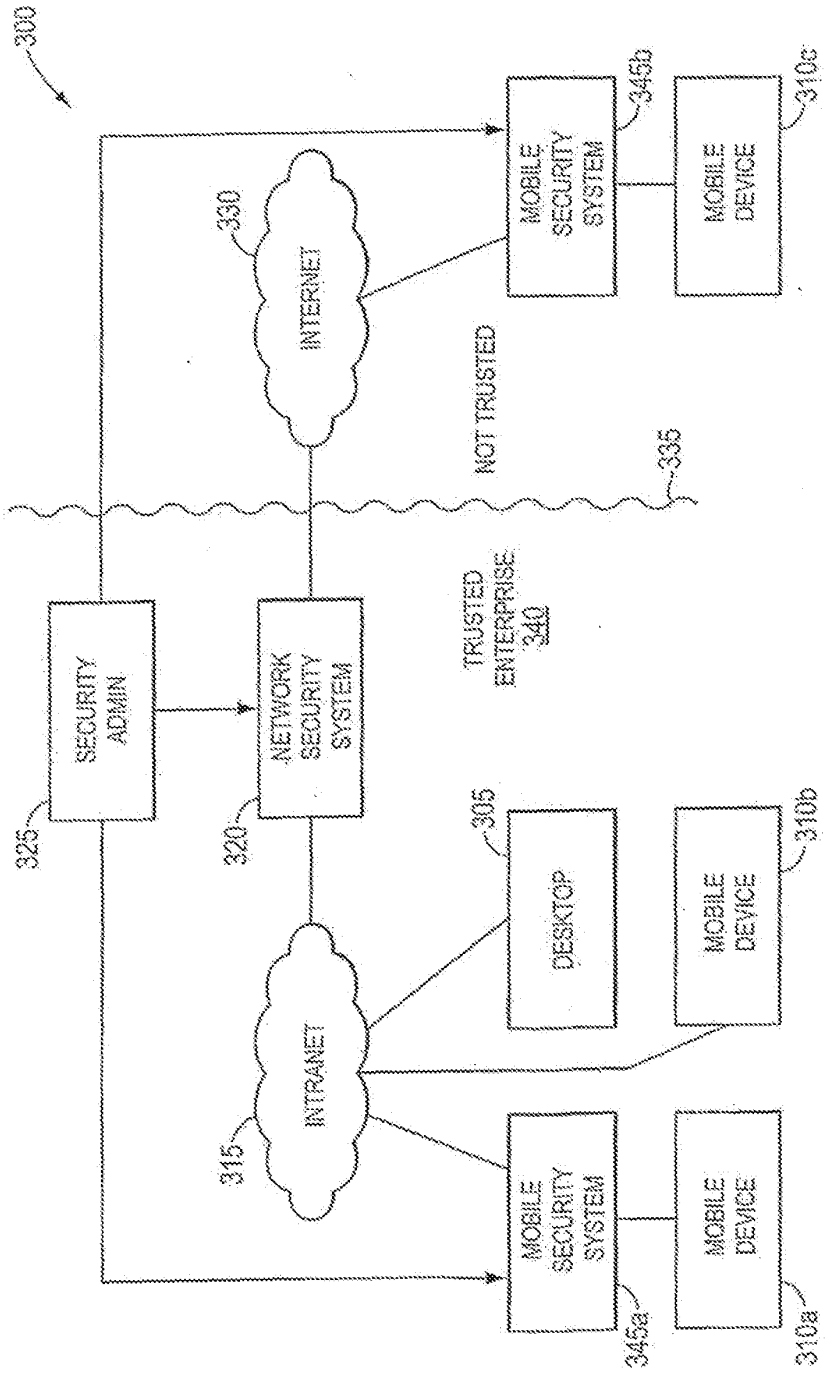

300
330
INTERNET
MOBILE SECURITY SYSTEM
345b
MOBILE DEVICE
310c
NOT TRUSTED
335
TRUSTED ENTERPRISE 340
SECURITY ADMIN
325
NETWORK SECURITY SYSTEM
320
305
DESKTOP
MOBILE DEVICE
310b
INTRANET
315
MOBILE SECURITY SYSTEM
345a
MOBILE DEVICE
310a

FIG. 3

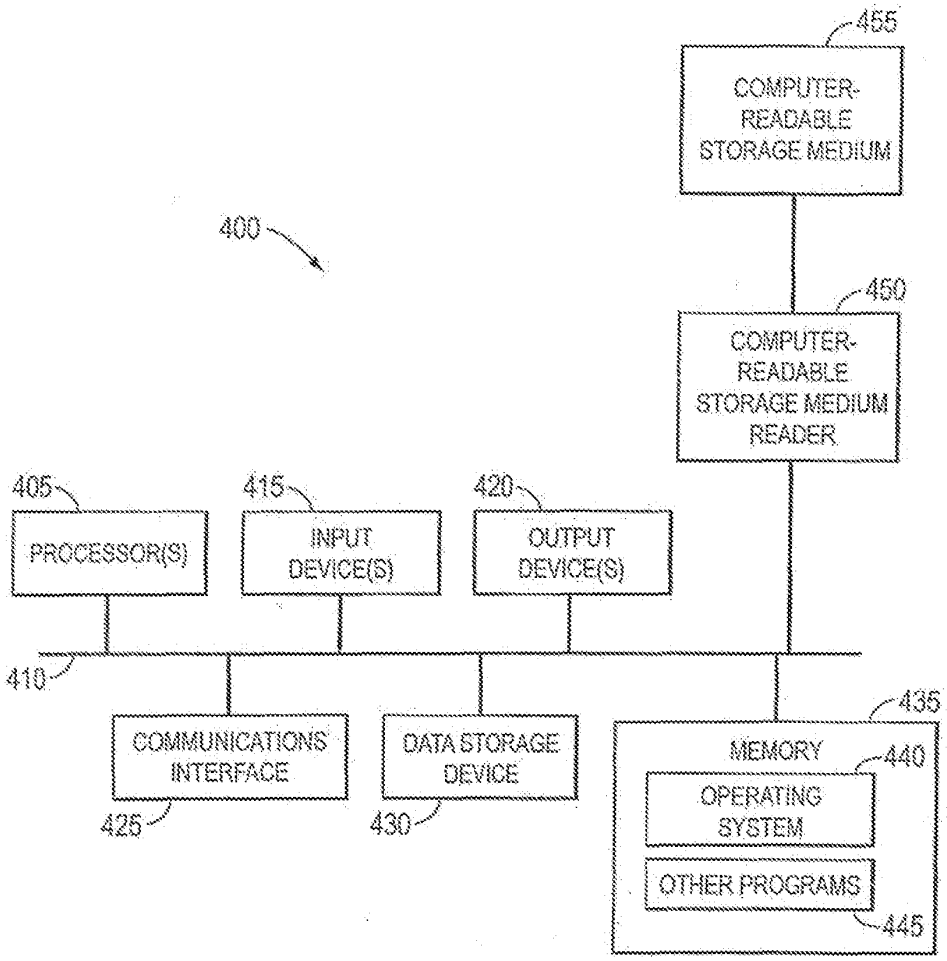

455
COMPUTER-READABLE STORAGE MEDIUM
400
450
COMPUTER-READABLE STORAGE MEDIUM READER
405
PROCESSOR(S)
415
INPUT DEVICE(S)
420
OUTPUT DEVICE(S)
410
COMMUNICATIONS INTERFACE
425
DATA STORAGE DEVICE
430
435
MEMORY
440
OPERATING SYSTEM
OTHER PROGRAMS
445

FIG. 4

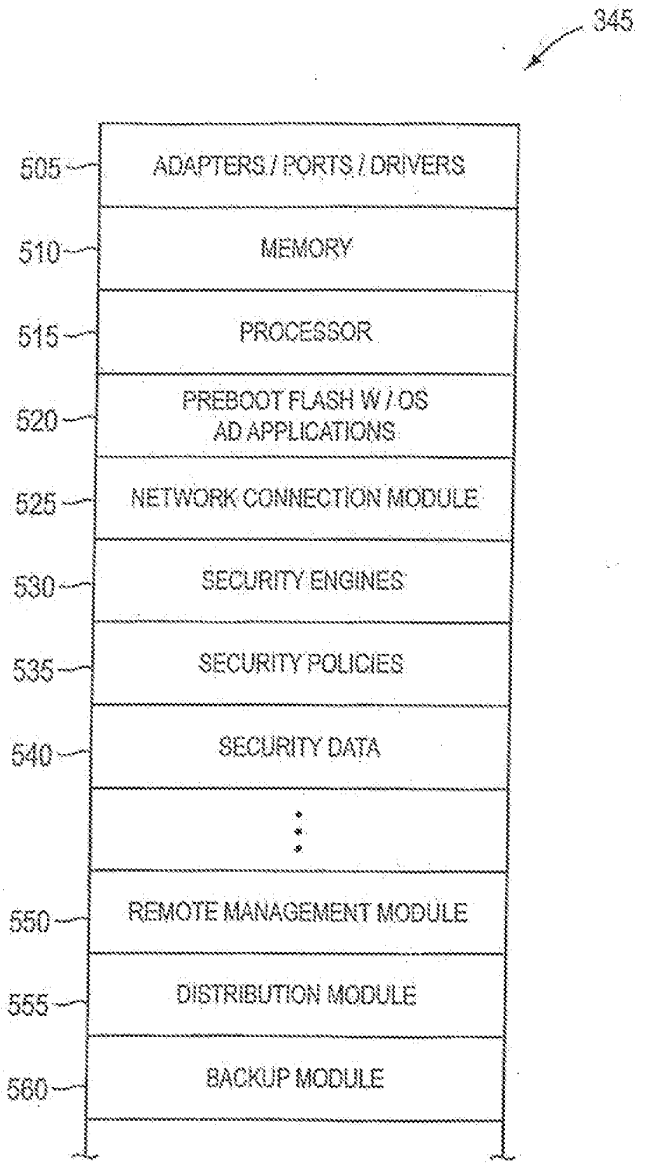

345
505
ADAPTERS / PORTS / DRIVERS
510
MEMORY
515
PROCESSOR
520
PREBOOT FLASH W / OS
AD APPLICATIONS
525
NETWORK CONNECTION MODULE
530
SECURITY ENGINES
535
SECURITY POLICIES
540
SECURITY DATA
550
REMOTE MANAGEMENT MODULE
555
DISTRIBUTION MODULE
560
BACKUP MODULE

FIG. 5

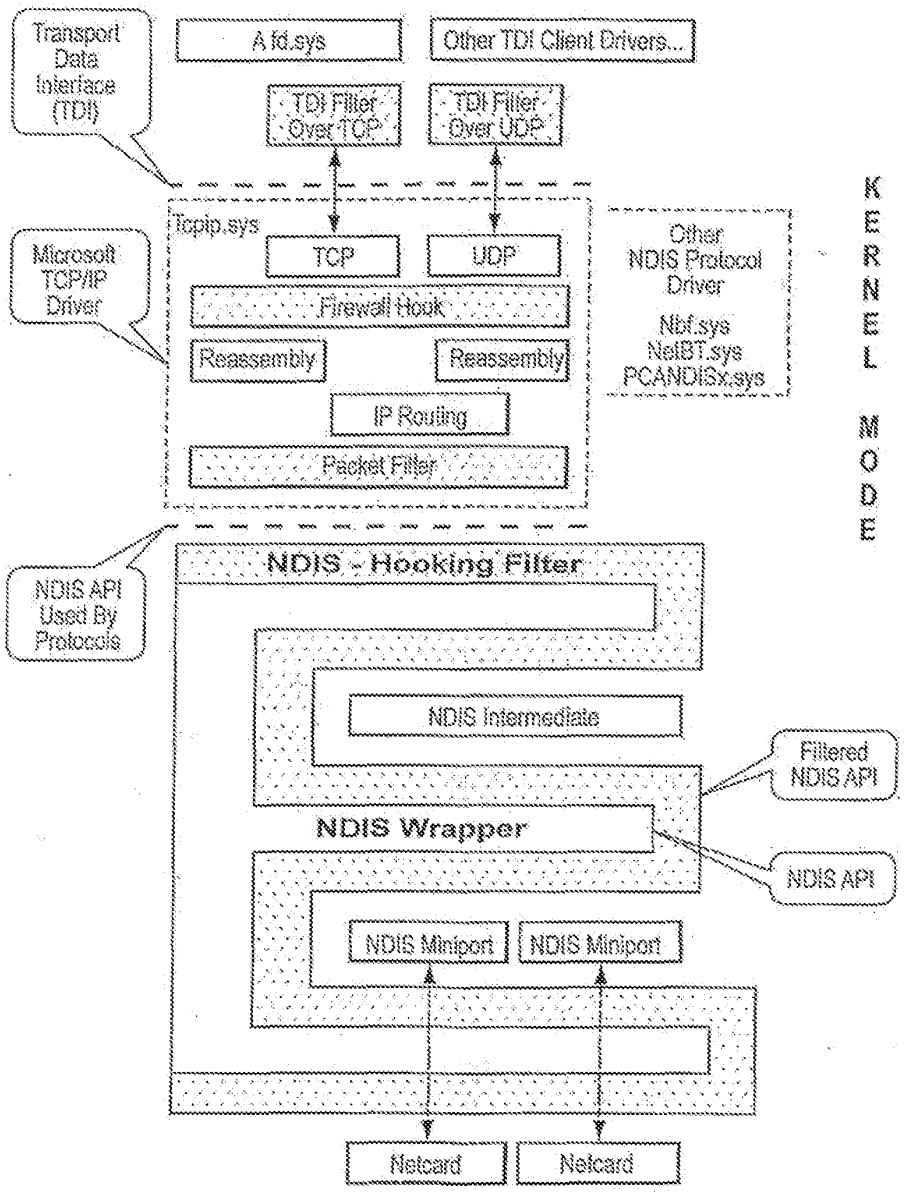

Transport Data Interface (TDI)
Afd.sys
Other TDI Client Drivers...
TDI Filter Over TCP
TDI Filter Over UDP
Tcpip.sys
TCP
UDP
Firewall Hook
Reassembly
Reassembly
IP Routing
Packet Filter
Microsoft TCP/IP Driver
Other NDIS Protocol Driver
Nbf.sys
NetBT.sys
PCANDIS.sys
KERNEL MODE
NDIS - Hooking Filter
NDIS API Used By Protocols
NDIS Intermediate
Filtered NDIS API
NDIS Wrapper
NDIS API
NDIS Miniport
NDIS Miniport
Netcard
Netcard

FIG. 6

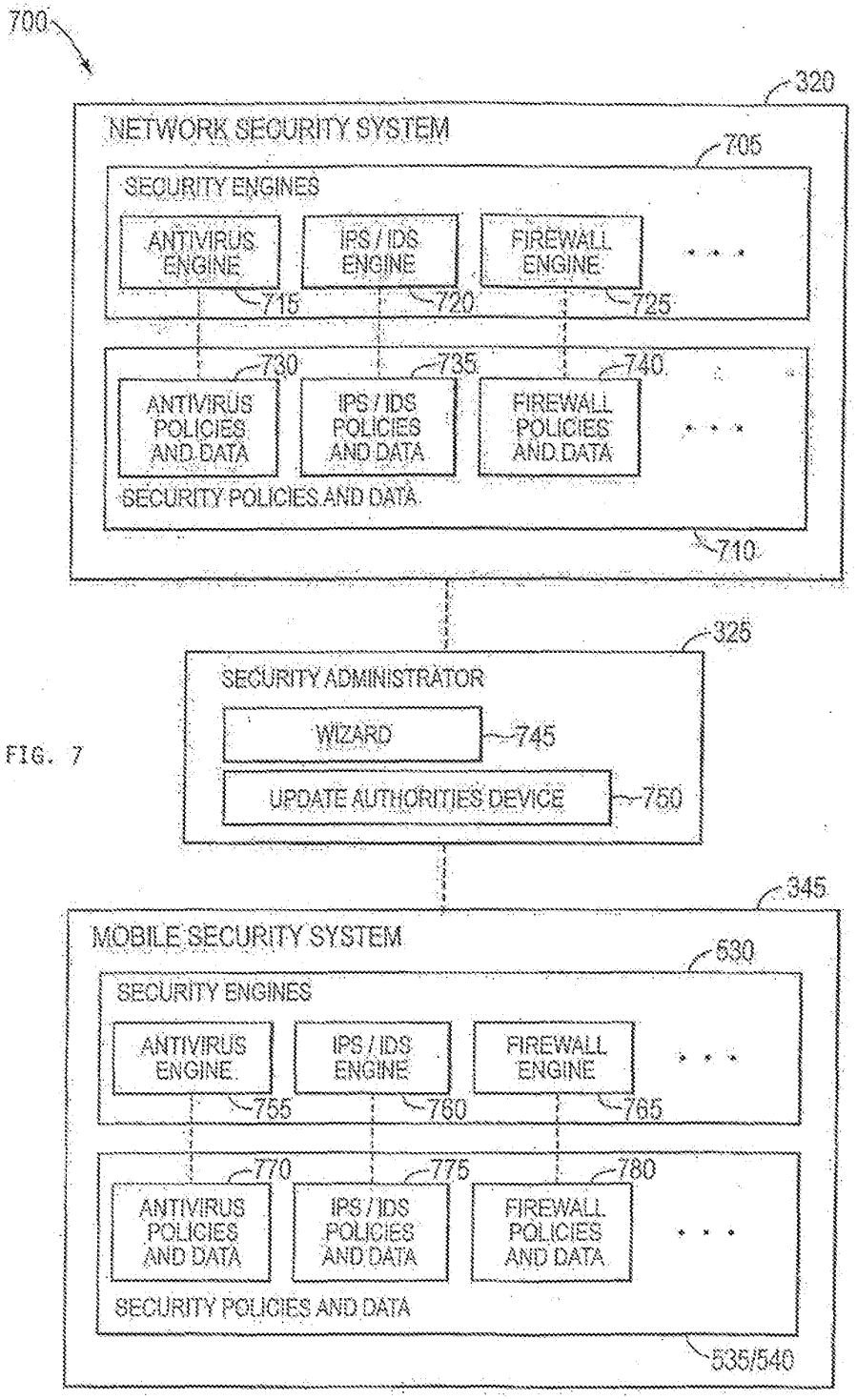

700
320
NETWORK SECURITY SYSTEM
705
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
715
720
725
730
735
740
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
710
325
SECURITY ADMINISTRATOR
WIZARD
745
UPDATE AUTHORITIES DEVICE
750
345
MOBILE SECURITY SYSTEM
530
SECURITY ENGINES
ANTIVIRUS ENGINE
IPS / IDS ENGINE
FIREWALL ENGINE
755
760
765
770
775
780
ANTIVIRUS POLICIES AND DATA
IPS / IDS POLICIES AND DATA
FIREWALL POLICIES AND DATA
SECURITY POLICIES AND DATA
535/540

FIG. 7

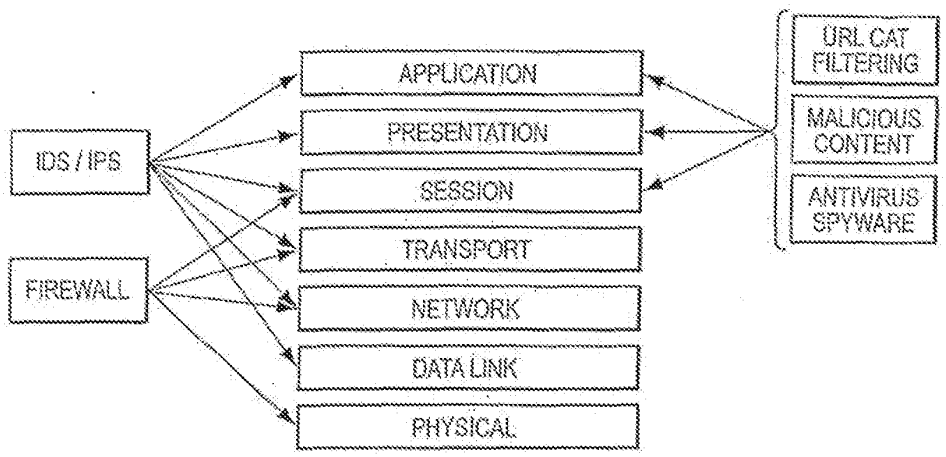

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL
IDS / IPS
FIREWALL
URL CAT FILTERING
MALICIOUS CONTENT
ANTIVIRUS SPYWARE

FIG. 8

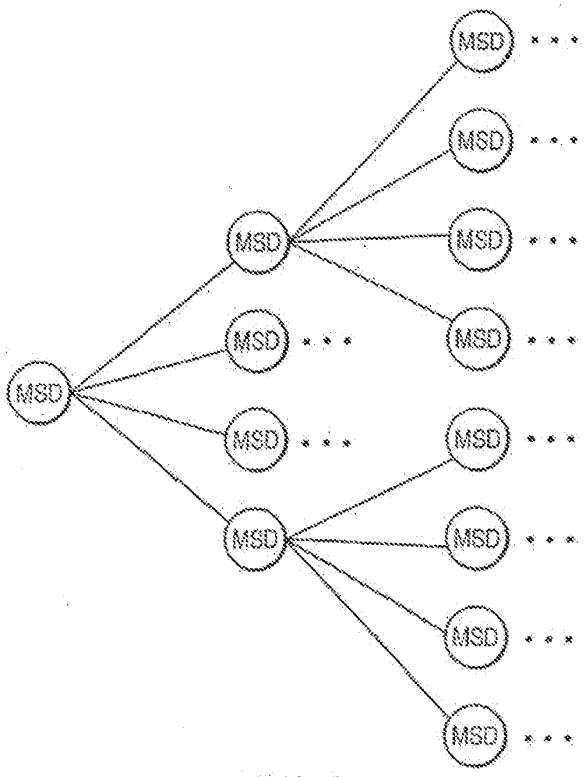

MSD

FIG. 9

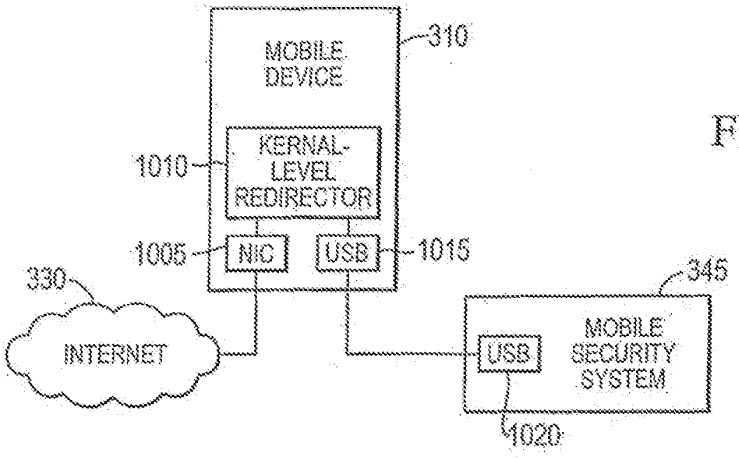


FIG. 10A

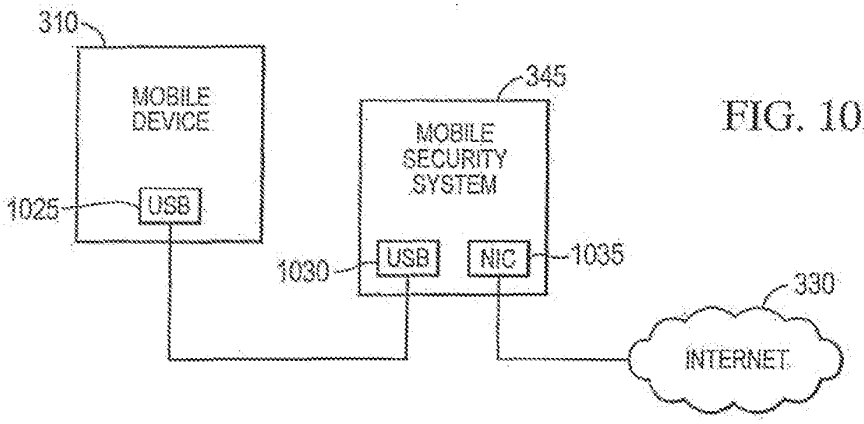


FIG. 10B

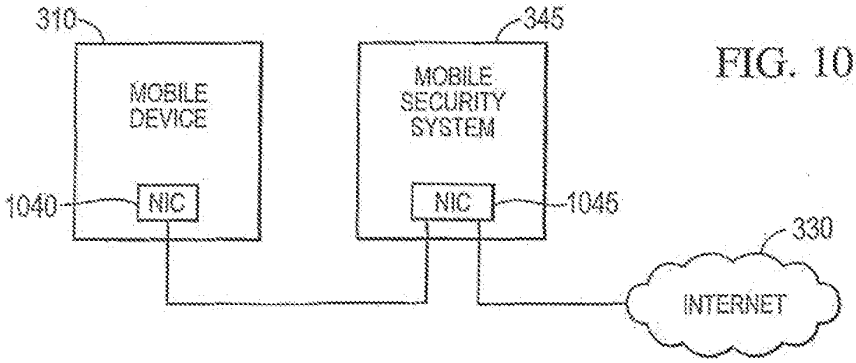


FIG. 10C

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2008 (05.06.2008)

PCT

(10) International Publication Number
WO 2008/066419 A1

(51) International Patent Classification:
H04Q 3/00 (2006.01) *H04L 12/24* (2006.01)

(21) International Application Number:
PCT/SE2006/001364

(22) International Filing Date:
29 November 2006 (29.11.2006)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LIDSTRÖM, Mattias** [SE/SE]; Kungsholms Kyrkoplan 3A, S-112 24 Stockholm (SE). **MATTI, Mona** [SE/SE]; Danielsvägen 2A, S-131 40 Nacka (SE). **KVERNVIK, Tor** [NO/SE]; Ropgränd 8, S-187 42 Täby (SE). **BJÖRK, Niklas** [SE/SE]; Krokivägen 13, S-175 47 Järfälla (SE). **LARSSON, Tony** [SE/SE]; Nils Ahlins väg 2, S-194 76 Upplands Väsby (SE). **BENITO GARCIA, Raul** [ES/ES]; C/Cordoba 7-4a, ES-28770 Colmenar Viejo (ES).

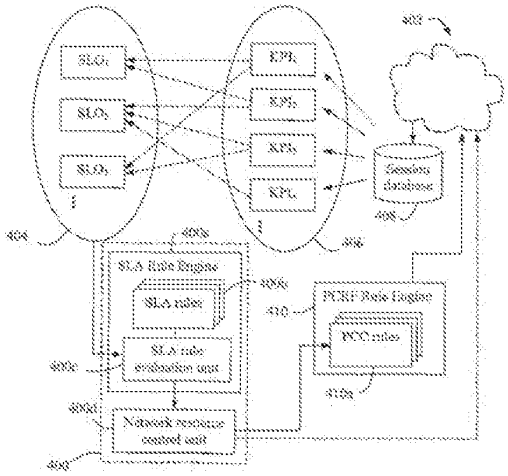
(74) Agent: **RAGSTÖM, Hans**; Bergenstråhle & Lindvall AB, Box 17704, S-118 93 Stockholm (SE).

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

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

Published:
— *with international search report*

(54) Title: A METHOD AND ARRANGEMENT FOR CONTROLLING SERVICE LEVEL AGREEMENTS IN A MOBILE NETWORK.



(57) Abstract: A method and an arrangement in a service assurance module (400) for controlling service level agreements for communication services in a mobile services access network (402). A network performance rule (400b) is created for a service level agreement, and is based on an associated performance indicator (406) indicating the current network performance with respect to the fulfilment of the service level agreement. The performance indicator is then monitored, and the network performance rule is evaluated on a regular basis based on the performance indicator. If the network performance rule is not satisfied, an agreement violation is registered and/or measures are taken to improve the network performance.

WO 2008/066419 A1

A METHOD AND ARRANGEMENT FOR CONTROLLING SERVICE LEVEL AGREEMENTS IN A MOBILE NETWORK.

TECHNICAL FIELD

The present invention relates generally to a method and arrangement for determining whether service level agreements are fulfilled in a mobile services access network. In particular, any quality-related problems in the network that may have a negative impact on service level agreements, may be detected and redeemed.

BACKGROUND

With the emergence of 3G mobile telephony, new packet-based communication technologies using IP (Internet Protocol) have been developed to support wireless communication of multimedia. For example, communication protocols in GPRS (General Packet Radio Service) and WCDMA (Wideband Code Division Multiple Access) support packet-switched multimedia services, as well as traditional circuit-switched voice calls.

A network architecture called "IP Multimedia Subsystem" (IMS) has been developed by the 3rd Generation Partnership Project (3GPP) as a platform for handling multimedia services and sessions in the packet domain, based on IP transport. Thus, an IMS network can be used to initiate and control multimedia sessions for IP enabled terminals being connected to any type of access networks. A signalling protocol called "SIP" (Session Initiation Protocol, according to the standard IETF RFC 3261) has been defined for handling sessions in IMS networks. A "SIP-enabled" terminal can thus use this standard to initiate and

terminate multimedia communications by means of its home IMS network.

Fig. 1 is a simplified schematic illustration of a basic network structure for providing multimedia services for a mobile terminal A by means of an IMS network 100. The terminal A is connected to a mobile access network 102 and communicates in a multimedia session with another terminal B which may be connected to the same access network 102 or another access network (not shown). Alternatively, terminal A may communicate with a content server or the like, e.g. for downloading some multimedia content therefrom.

The access network 102 is connected to IMS network 100 which is the "home" IMS network of terminal A and therefore handles the session with respect to terminal A. The same IMS network 100 or another one (not shown), may handle the session on behalf of terminal B. Moreover, multimedia services are always handled by the terminal's home IMS network even if terminal A would be roaming in a visited access network.

The session is controlled by specific nodes in the IMS network 100, here generally referred to as "session managing nodes" 104. These nodes include S-CSCF (Serving Call Session Control Function), I-CSCF (Interrogating Call Session Control Function) and P-CSCF (Proxy Call Session Control Function, according to the conventional IMS architecture. Briefly described, a P-CSCF node acts as an entry point towards the IMS network 102 from access networks, including network 100, a plurality of S-CSCF nodes are assigned to active terminals for managing their sessions using SIP signalling, and an I-CSCF node acts as a gateway for SIP messages from other IMS networks.

The IMS network 102 also includes one or more application servers 106 for enabling various multimedia services, and a main database element HSS (Home Subscriber Server) 108 containing subscriber and authentication data. The various functions of the shown network elements 104-108 are generally known in the art, and not necessary to describe here further to understand the context of the present invention. Of course, IMS network 102 contains various other nodes and functions not shown here for the sake of simplicity. In the figure, the thick two-way arrow illustrates the communication of payload data between the two terminals A, B. The thin two-way arrow illustrates the communication of control messages, typically according to SIP in the case of IMS.

A policy unit 110 associated with the access network 102 is also connected to the IMS network 100. The policy unit 110 is basically responsible for authorising communication sessions for terminals connected to the access network 102, based on various predetermined policies and rules. The policy unit 110 generally operates according to a function implemented therein called PCRF (Policy and Charging Rule Function), sometimes alternatively referred to as PDF (Policy Decision Function).

The PCRF uses a rule engine that evaluates session information related to a requested session, in order to determine whether the session can be allowed or not. A session may be allowed conditionally, e.g., "session X is allowed if condition Y is met". Session admission rules defined in the rule engine of policy unit 110 specify when to allow sessions for specific users and/or services. The rules can be combined into policies which may be defined for specific users or services, or both. When a session request

is received from a user for a specific service, a relevant policy or rule combination is thus selected and evaluated for the session request for allowance or rejection.

Many mobile applications and services require a certain Quality of Service QoS in order to provide a satisfying and expected result to end-users. For UMTS networks, four main traffic classes have been defined: "conversational class", "streaming class", "interactive class" and "background class", in order to classify different needs and requirements regarding bit rates and delays. These traffic classes are primarily distinguished by their requirements regarding transfer delays, such that applications of the conversational class tolerate only small delays, sometimes also referred to as "real-time", whereas the background class is applied to the least delay-sensitive applications, sometimes also referred to as "best effort".

The selection of a UMTS traffic class for an application is used for assigning a suitable physical channel in the mobile network, generally referred to as a RAB (Radio Access Bearer), in order to optimise the scarce radio recourses and other transport resources in the radio access and core networks whilst maintaining an acceptable and expected level of quality for the end-user.

Another factor that may dictate the QoS requirements is the subscription type. Thus, subscribers may be offered specific service levels with respect to QoS for different subscription types. For example, using current terms, a "Platinum" subscription may be defined to guarantee a relatively high level of service or QoS, whereas "Gold", "Silver" and "Bronze" subscriptions may provide successively lower levels of service or QoS. Moreover, specific services

may also be offered with different levels of QoS, e.g. at different prices.

Fig. 2 illustrates a conventional process when a mobile terminal A will communicate multimedia with another party B, involving different **stages 2:1 - 2:9** as illustrated. Here, each stage may generally represent the communication of various messages and/or data back and forth which are not necessary to describe in more detail.

IMS nodes P-CSCF 202 and S-CSCF 204 are shown here in a schematic "control plane" for control signalling over the IMS network. Further, a gateway node GW 200 in the core part of a mobile network, typically a GGSN (Gateway GPRS Switching Node), is shown in a schematic "bearer plane" used for the data transport. The gateway node GW 200 is connected to an associated policy unit 206, here denoted PCRF, which is thus basically responsible for authorising communication sessions to terminals in the associated mobile network, as described above. In some systems, a so-called "Policy and Charging Enforcement Function" (PCEF) in the GGSN node typically communicates with the PCRF node over a Gx interface to control the access admission, and the PCRF node communicates with the P-CSCF node over an Rx interface.

In a first **stage 2:1** of the illustrated procedure, terminal A obtains an initial connection with the mobile network, typically involving the activation of a PDP context and a Radio Access Bearer RAB, as established by the gateway node GW 200. A particular PCRF 206 is also selected for terminal A by GW 200 at this point. The established access bearer is primarily used for carrying occasional control messages of minor size such as service requests, allowing for relatively low bandwidth and fairly long delays.

In a next **stage 2:2**, GW 200 sends relevant access information to PCRF 206, including a subscription identifier and the bearer information established in stage 2:1. Thereby, a "state" is created in PCRF 206 for a "bearer session", meaning that the received access information for terminal A is retained in PCRF 206. In this stage, PCRF 206 also responds to GW 200 by sending a so-called "basic charging rule" that has been selected or created based on the received access information. The basic charging rule includes a charging key, a charging identity and any service data flow filters that should be applied on communicated data according to that rule. A certain basic level of QoS, typically the "best effort" level, has now also been established for non-IMS data services such as the communication of various control messages as mentioned above.

When a user activates a selected application in terminal A in order to communicate with terminal B in this case, an SIP-based user agent ("SIP UA") in terminal A performs a session negotiation in a following **stage 2:3**, which may involve the exchange of terminal capabilities with terminal B. In the session negotiation, terminal A may start by sending an SIP INVITE message as a session request towards terminal B containing session-specific parameters typically including a proposed coder/decoder (or "codec") for the session.

After the session negotiation, as the session parameters have been settled, the P-CSCF node 202 sends corresponding service information to PCRF 206, in a next **stage 2:4**. Thereby, another state is created in PCRF 206 for a "service session", meaning that the received service information for the session of terminal A is retained in

PCRF 206. Moreover, PCRF 206 determines whether the requested session should be allowed or not by applying a suitable policy.

If PCRF 206 can allow the requested session according to the applied policy for the given user and service, an OK message is sent to the P-CSCF node 202 which also sends an OK message to the terminal A, in a **stage 2:5**. The application activated in terminal A then requests a bearer from a bearer part in terminal A, in a following **stage 2:6**, in order to satisfy QoS requirements for communication according to the application. Terminal A then issues a bearer request for service data transport to GW 200 in the mobile network, in a next **stage 2:7**. Alternatively, the establishment of bearer may also be initiated by the mobile network.

In a further **stage 2:8**, GW 200 now establishes a new bearer for the forthcoming data transport, as required by the service, and sends relevant QoS information on the established service bearer to PCRF 206 where the bearer session state is updated accordingly. In this stage, PCRF 206 also responds to GW 200 by sending an updated charging rule based on the received service and QoS information. The updated charging rule includes a service identity, a charging identity and any service data flow filters according to that rule. Hence, a certain level of QoS has also been established for the requested service, typically a higher QoS level than the one established for non-IMS data services in stage 2:2 above.

The above-mentioned basic charging rule and updated charging rule established for terminal A in stages 2:2 and 2:8, respectively, are often referred to as "PCC (Policy and Charging Control) rules", in effect being rules for session

admission. In general, a PCC rule is used for detecting packets belonging to a service data flow, identifying the service, and for providing relevant charging parameters and policy control for a data flow. A PCC rule may be predefined or created dynamically, and includes basically a rule name, a service identifier, service data flow filters, QoS parameters and charging parameters.

Finally, terminal A can start the session involving the communication of data between the two terminals A and B, as illustrated by a final **step 2:9**. The new service bearer or RAB established in stage 2:8 should be more stable and reliable than the access bearer established for control messages in stage 2:2, to provide a "guaranteed" level of QoS according to the service involved as controlled by the updated charging rule. As mentioned above, different levels of QoS may also be expected depending on the subscription and/or selected level of service.

However, the mobile network will undoubtedly sometimes fail to fulfil the agreed level of QoS during such sessions. The reasons for not providing the agreed levels of service can be many, often depending on the current traffic situation such as cell congestion and interference problems, but also on factors related to the operation of the network such as inadequate power regulation, equipment failure, inaccurate channel allocation and poor radio coverage, etc.

Today, there is no efficient way to monitor service level agreements in mobile networks, and consequently it cannot be controlled that these agreements are met properly. Hence, if a customer complains that an expected QoS level has not been fulfilled during a session, the network operator has no means to check the relevance thereof. Moreover, the operator cannot work proactively to ensure

that service level agreements are fulfilled. Instead, a reactive process must be used for investigating a network in order to identify such problems and where they typically occur. This is an expensive and time consuming activity that nonetheless must be undertaken in order to improve the fulfilment of service agreements, and to avoid customer dissatisfaction and the paying of resulting penalty fees.

SUMMARY

It is an object of the present invention to address the problems outlined above. More specifically, it is an object of the present invention to make it possible to detect and identify any performance shortcomings that may jeopardise service level agreements in a mobile services access network, in order to take suitable measures to remedy such deficiencies.

These objects and others can be obtained by providing a method and an arrangement according to the independent claims attached below.

According to one aspect, the present invention involves a method of controlling a service level agreement for a communication service in a mobile services access network. The method includes creating a network performance rule valid for the service level agreement and being based on an associated performance indicator indicating the current network performance with respect to the fulfilment of the service level agreement. The method further includes monitoring the performance indicator and evaluating the network performance rule based on the monitored performance indicator. An agreement violation is then registered and/or measures are taken to improve the network performance, if the evaluated network performance rule is not satisfied.

According to another aspect, the present invention also involves a service assurance module in a mobile services access network for controlling service level agreements for communication services. The service assurance module comprises means for creating a network performance rule valid for a service level agreement and being based on an associated performance indicator indicating the current network performance with respect to the fulfilment of the service level agreement. The service assurance module further comprises means for monitoring the performance indicator, means for evaluating the network performance rule based on the monitored performance indicator, and means for registering an agreement violation and/or for taking measures to improve the network performance, if the network performance rule is not satisfied.

The invented method and service assurance module may optionally have the following further characteristics.

The measures to improve network performance may include modifying or adding a session admission rule applied for individual terminals and session requests, to introduce access constraints. The session admission rule is then used by a rule engine of a policy unit to control the admission of individual sessions.

The network performance rule may include a degradation rule specifying a degradation level of the monitored performance indicator, and a violation rule specifying a violation level of the monitored performance indicator when the service level agreement is deemed to be violated. The degradation and violation rules are conditional by dictating said measures to improve network performance if the respective rule is not met, and the

violation rule is evaluated if the degradation rule is not satisfied.

The network performance rule may be dependent on a plurality of associated performance indicators indicating different aspects of the current network performance with respect to the fulfilment of the service level agreement.

The monitored performance indicator(s) may be derived from a session database used by the mobile network and may relate to any of: bandwidth occupation, latency, packet loss rate, available bitrate, or network and service accessibility.

The present invention makes it possible to create specific service level agreements for individual services and/or subscribers, and to ensure that these agreements can be substantially satisfied. Performance problems occurring in a network can also be identified and located, by means of monitored performance indicators declared in network performance rules. Thereby, the network operator can work proactively in order to avoid the violation of service level agreements.

Further features of the present invention and its benefits will be explained in the detailed description below.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail by means of preferred embodiments and with reference to the accompanying drawings, in which:

- Fig. 1 is a schematic communication scenario of a multimedia session between two mobile terminals A and B using a conventional IMS network, according to the prior art.

- Fig. 2 illustrates a conventional signalling flow during the establishment of a session between terminals A and B using a policy unit PCRF, according to the prior art.
- Fig. 3 is a diagram illustrating the fluctuations of a monitored network performance indicator over time.
- Fig. 4 is a block diagram illustrating the operation of a network performance rule engine connected to a session admission rule engine, according to one embodiment.
- Fig. 5 is a flow chart illustrating a procedure for overseeing service level agreements in a mobile services access network, according to another embodiment.
- Fig. 6 is a flow chart illustrating a procedure for controlling network resources in a mobile services access network based on at least one monitored performance indicator, according to another embodiment.

DETAILED DESCRIPTION

Briefly described, the present invention involves a service assurance module or similar including a "network performance rule engine", referred to as the "SLA rule engine" for short in the following description, which can be used to improve the fulfilment of service level agreements (SLA) in a mobile services access network. The SLA rule engine is thus used for monitoring whether such agreements are satisfied, based on network performance rules that have been derived or translated from the agreements, and can also be used for controlling network resources to remedy or avoid any violations thereof.

The SLA rule engine is connected to the above-described session admission rule engine in the policy unit PCRF, hereafter referred to as the "PCRF rule engine". Thus, whereas the session admission rules in PCRF (i.e. PCC rules)

are applied for individual terminals and session requests to control session admission, the network performance rules in the SLA rule engine are evaluated with respect to network performance for subscriber groups and/or specific services, which in turn depends on the outcome from the PCRF rule engine. Hence, the results from the SLA rule engine indicate the extent of service level agreement fulfilment. The outcome from the SLA rule engine can then be used for detecting any overloading or deficiencies in the mobile network, and for improving the network performance by controlling network resources, in a manner that will be described below by means of exemplary embodiments.

The rules in the SLA rule engine may be frequently evaluated on a regular basis, e.g. at intervals of five minutes. An SLA rule may specify a maximum period of time during which an SLA violation can be tolerated, which of course will depend on the nature of agreement and service. In other words, in may be deemed acceptable that an SLA is violated temporarily, as long as it is fulfilled again within the set time period.

In order to determine whether an SLA is fulfilled or not, one or more performance indicators are monitored, hereafter referred to as the "Key Performance Indicator", KPI. A KPI generally indicates the performance in the network with respect to a predefined factor or parameter relevant for an evaluated SLA rule, that can be detected or measured to determine a current KPI value or level, which typically fluctuates over time.

The KPI values may be derived from information in a session database maintained in the mobile network, but also from other information sources, and the present invention is not limited in this respect. For example, a KPI

may relate to bandwidth occupation, latency, packet loss rate, available bitrate, or network and service accessibility, etc., although the present invention is not limited to these examples neither. Thus, a plurality of KPI's related to different aspects of network performance may be monitored in order to evaluate rules in the SLA engine and ultimately the fulfilment of service level agreements.

Fig. 3 is a schematic diagram of an exemplary performance indicator KPI being monitored, where the horizontal axis represents time and the vertical axis represents the KPI level. In this example, the KPI is related to the occupation of bandwidth in a certain area such as a cell or group of cells in a mobile network, and/or for a specific service. The curve 300 thus represents the measured KPI over time. In general, the KPI level is high when a large percentage of the available bandwidth is occupied, and vice versa.

In this case, a violation level of the KPI has been predefined, as indicated in the figure. Basically, a service level agreement SLA ensuring a certain amount of free bandwidth in the monitored area and/or service, will be violated if the KPI value exceeds the violation limit for more than a predetermined maximum acceptable time period T. Further, a relatively lower KPI level has also been defined over which the bandwidth availability is considered to be degraded, as indicated in the figure.

As can be seen in the figure, the fluctuating KPI stays below the degradation level until the time t_1. Thereafter, the KPI exceeds the degradation level, and the KPI increases further to even exceed the violation level at the time t_2. In this case, the violation level has been

exceeded for more than the maximum acceptable time period T after the time t_3, until the KPI decreases to fall below the violation level at the time t_4, and finally also below the degradation level at the time t_5. Hence, a service level agreement being dependent on the KPI depicted in Fig. 3 is considered to be violated during the period between t_3 and t_4, i.e. after the maximum acceptable time period T.

In the example above, as soon as the KPI level rises above the degradation level after t_1, it is possible to determine why and where the degradation has occurred, as indicated by the KPI. Thereby, suitable measures can be taken in the mobile network at some point after t_1 to control network resources, in order to remedy the problem and improve the bandwidth availability such that the KPI level does not rise further to unacceptable levels. For example, the KPI results can be used for modifying and/or adding selected PCC rules to control the bandwidth occupation, e.g., by introducing access constraints or the like in the PCC rules. Thus, once the KPI becomes degraded, session admission may be denied or restricted for certain services and/or subscribers in order to improve the bandwidth availability for other services and/or subscribers with higher priority.

In this way, the performance problem can be redeemed proactively by controlling network resources, such that the KPI level is kept within acceptable limits, as indicated by an exemplary dashed curve 302 in Fig. 3. Violation of the associated SLA can then be avoided or at least reduced.

In order to evaluate the fulfilment of service level agreements in a mobile network, different "Service Level Objectives" (SLO) may be defined based on monitored

performance indicators (KPI), such that one or more specific performance indicators are associated with each service level objective. Thus, a service level objective SLO is basically deemed to be fulfilled as long as no associated performance indicator KPI exceeds a predefined violation level for more than a maximum acceptable time period.

Fig. 4 illustrates schematically the operation of a service assurance module 400 comprising an SLA rule engine 400a, according to one embodiment. In the SLA rule engine 400a, one or more SLA rules 400b (i.e. network performance rules) have been defined to evaluate the network performance with respect to SLA's (i.e., service level agreements) for subscribers and/or services in a mobile services access network 402.

A plurality of service level objectives 404 have also been defined for the SLA rule engine 400a, each being dependent on one or more performance indicators 406. An SLA rule may basically involve one or more SLO's. In this example, a first service level objective SLO_1 is associated with performance indicators KPI_1 and KPI_2. Further, a second service level objective SLO_2 is associated with performance indicators KPI_2, KPI_3 and KPI_4, and a third service level objective SLO_3 is associated with performance indicators KPI_1 and KPI_4, respectively.

The SLA rule engine 400 further includes a rule evaluation unit 400c receiving KPI measurements for each SLO 404, which is adapted to evaluate the SLA rules 400b based on the received KPI measurements. The mobile network 402 and the subscribers and services therein effectively constitute the environment in which the measured KPI's are formed. The KPI's 406 may be derived from a session database 408 used by

the network 402, as illustrated by arrows, but also from other sources of network information, not shown.

The service assurance module 400 further comprises a resource control unit 400d adapted to generally control network resources, in response to the evaluation of the SLA rules in the evaluation unit 400c. A conventional PCRF rule engine 410 is used by the mobile network 402 to control session admission for its subscribers and services, and the network resource control unit 400d is connected thereto. The control unit 400d is further adapted to modify and/or add PCC rules 410a in the PCRF rule engine 410 in response to the SLA rule evaluation, to control resources in network 402 such that any SLA violations can be avoided or at least reduced, as described above.

The control unit 400d may also be adapted to influence resources and operations in network 402 in other ways, as schematically indicated by the dashed arrow. For example, channel allocation schemes, power regulation and radio coverage, etc., may be modified in response to the evaluation of SLA rules using methods and routines well-known to the skilled person.

It should be noted that the arrangement depicted in Fig. 4 is purely logical and can be implemented in different ways. For example, the SLA rule engine 400a and the network resource control unit 400d can be arranged together as the shown service assurance module 400, but may also be arranged as separate connected entities. The components 400a-d in the shown service assurance module 400 may further be integrated with the PCRF Rule Engine 410, or implemented as a separate connected module, node or system. An Operation and Maintenance (O/M) interface (not shown) to the SLA rule engine 400a may be used allowing an Operation

and Support System (OSS) to supervise the fulfilment of SLA's, and providing the possibility to operators in a Network Operation Centre (NOC), to modify parameters in SLA Policies to control SLA fulfilment.

As shown by means of various arrows, the arrangement in Fig. 4 basically produces a network control "loop" for optimising the usage of network resources in order to fulfil prevailing SLA's. Thus, the session database 408 (and possibly also other information sources, not shown) provides KPI values 406, associated with different SLO's 404. The evaluation unit 400c evaluates the SLA rules based on the obtained KPI values and the associated SLO's, and the outcome is used by the network resource control unit 400d to modify and/or add PCRF rules 410a (and possibly also to influence the network 402 in other ways, as indicated by the dashed arrow), if necessary. As a result, the network 402 will provide a different performance, as reflected in the session database 408 and otherwise, such that the measured KPI's 406 hopefully become improved.

Fig. 5 is a flow chart of steps executed by a service assurance module or similar, adapted to oversee service level agreements in a mobile services access network and control network resources such that violations of the service level agreements can be avoided or at least reduced. In a first **step 500**, a network performance rule is created based on one or more service level agreements valid for the mobile network. At least one associated performance indicator is monitored in a next **step 502**, the level of which indicating whether any of the created service level agreements is fulfilled or not.

In a following **step 504**, it is determined whether the network performance rule is satisfied or not, based on

the monitored performance indicator(s). If the rule is satisfied, the process returns to step 502, such that steps 502 and 504 are repeated on a regular basis, e.g. at intervals of five minutes.

However, if the network performance rule is not satisfied in step 504, some different options are possible for the next **step 506**. One option is that a failure or breach of the service level agreement associated with the created network performance rule can be simply registered or logged in a database or the like, e.g. in order to collect SLA statistics. Another option in step 506 is that suitable measures are taken to somehow improve the network performance as relevant to the evaluated network performance rule, in response to a negative outcome of step 504, in order to influence the environment of the mobile network in a way that the service level agreement can be safely met again. For example, at least one session admission rule can be modified or added in a PCRF rule engine or similar, e.g. as described for Fig. 4 above. As indicated in step 506, either or both alternatives are possible.

As mentioned above in connection with Fig. 3, two different network performance rules may be set for a particular performance indicator, which can be used for controlling network resources in an mobile network to avoid or reduce any violation of the corresponding SLA. A first "degradation" rule specifies a degradation level or limit of the KPI as described for Fig. 3. The degradation rule is also "conditional" by dictating measures to be taken for changing the admission of sessions in order to remedy the network performance degradation, if the rule is not met. Further, a second "violation" rule specifies a violation level or limit of the KPI when the network performance has

deteriorated so that a service level agreement is deemed to be violated, e.g. when the violation limit is exceeded for more than a predetermined time period. The violation rule is also "conditional" in the same manner.

Fig. 6 is a flow chart illustrating a procedure for controlling network resources proactively in a mobile services access network, according to another embodiment, by using the above-mentioned degradation and violation rules created for a prevailing SLA, to avoid or at least reduce the violation of that SLA. The following example is concerned with only one performance indicator KPI and one session admission rule, even though the present invention is not limited in this respect but can be used for any number of performance indicators, session admission rules, network performance rules and service level agreements.

It is assumed that a degradation rule and a violation rule has been created with respect to a certain SLA as described above. In a first illustrated **step 600**, a performance indicator KPI is monitored, being relevant for the two network performance rules. In a next **step 602**, the degradation rule is evaluated to determine whether it is met or not, according to the monitored performance indicator. As long as the degradation rule is satisfied, it is still evaluated on a regular basis as described above, thus repeating steps 600 and 602 frequently.

However, if the degradation rule is not satisfied in step 602, a session admission rule is modified or added, in a **step 604**, hopefully impacting the monitored performance indicator. The session admission rule (i.e. PCC rule) may reside in a PCRF rule engine implemented in a policy unit controlling session admission for individual session requests in the mobile network, as shown in Fig. 4. The

degradation rule may thus dictate that if the KPI exceeds the degradation level or limit, the session admission rule should be modified in a specific way. For example, if the monitored performance indicator is bandwidth usage for service X, the degradation rule may dictate: "if the allocated bandwidth for service X exceeds 60%, downgrade bandwidth 1 level for Bronze subscribers".

Once the session admission rule has been modified or added, the performance indicator hopefully changes to the better, which is monitored further in a following **step 606**. It is then determined whether the violation rule is satisfied in a further **step 608**. If so, the process may return to the initial steps 600 and 602 to find out whether the performance indicator has improved such that the degradation rule is now also met.

However, if neither the violation rule is satisfied in step 608, an SLA violation may be registered or logged in a suitable database or the like, as indicated by an optional **step 610**. In any case, a session admission rule is once again modified or added, by returning to step 604. At this stage, the session admission rule modified or added previously in step 604 may be further modified this time, e.g. by introducing harder access constraints or the like. However, any other session admission rule could be modified or added, depending on the implementation, and the present invention is not limited in this respect.

The violation rule evaluated in step 608 may thus dictate that if the KPI exceeds the violation level, the previously modified or added session admission rule should be modified further. For example, if the degradation rule example given above has been used for steps 602 and 604, the violation rule may dictate: "if the allocated bandwidth for

service X exceeds 80% for more than 5 minutes, deny access for Bronze subscribers".

It is possible to define network performance rules in many different ways, based on various performance indicators. As mentioned above, conditional degradation and violation rules may dictate different measures to be taken when the rules are not met, in order to remedy or avoid the network performance problems. As mentioned above, these measures may include measures taken on various network operational tools and methods, but involve primarily the modification or addition of session admission rules which will typically produce a swift result. For example, a frequently used service with short lived sessions can be targeted for enforcing restrictions since the effects will be instant in that case.

When it is determined that a conditional network performance rule is met again, after having introduced a restriction by modifying or adding a session admission rule according to the above, the situation may be restored by removing the restriction, e.g. after a predetermined delay period and/or when the monitored KPI falls below a certain level. The evaluated network performance rule may specify how and when a previously introduced restriction is to be removed.

More or less complex rule schemes may be created where different services affect each other. For example, a conditional degradation rule may dictate that if the allocated bandwidth for service X exceeds a certain limit, agreements on services X, Y and Z cannot be fulfilled for Platinum users, and therefore the access to one or more of these services is restricted for Bronze users.

Different service level agreements between a network operator and subscribers will be given different priorities, and different performance indicators KPI's can be given different priorities within each service level agreement as well. Using the present invention, it is therefore possible to create specific service level agreements for individual services and subscribers or subscriber groups, also ensuring that the agreements can be satisfied. The invention also provides a solution to identify any performance problems in a network and where they occur, since each KPI declared in the network performance rules can be monitored easily and efficiently. The network operator can thus work proactively in order to enhance service offerings and ultimately the end user experience.

The present invention may be implemented and configured as follows: SLA rules for one or more subscriber groups or categories may be created in connection with introducing a service. The service will thus have policies that are derived from the SLA which may be offered along with the service. These policies are made up of session admission rules (PCC rules) set in the PCRF rule engine and network performance rules (SLA rules) set in the SLA rule engine.

The PCC rules are focused on the single user and dictates how well a service will perform for the given user. On the other hand, the SLA rules are focused on how the service performs in the network, e.g. for a certain subscriber group or class, and how well the service performance matches the SLA between a service provider and an operator. The SLA rules are generally fewer than the PCC rules and require little effort from the operator of the

system to install. Since an SLA rule is valid for a subscriber group (i.e., a large aggregated group of end-users), the number of such rules will be limited.

The fact that the PCC and SLA rules focus somewhat differently allows for different outcomes when changing either of the two. When the SLA rules operate on the PCRF policies by impacting the PCC rules as described above, both QoS and SLA fulfilment can be assured. Initially, a network operator would probably prefer to use the SLA rule engine only for "important" customers that actually have SLA's with the operator such as corporate customers and services. The present invention also enables the possibility for an operator to use the SLA rule engine to provide important feedback for subscribers and services based on various groupings that the operator is free to define.

Thus, the following useful characteristics may generally be obtained when using the present invention:

- An SLA can be expressed in terms of concrete rules.
- An SLA and the service performance can be easily but carefully monitored by frequently evaluating the corresponding SLA rule.
- The network performance and the end user experience can be enhanced proactively.
- The operator's revenue can hopefully be increased.
- The amount of incoming complaints to a service/support desk (helpdesk) or the like can be reduced.

Moreover, As soon as the SLA rule engine outcome gives rise to a change of existing admission rules for any

subscriber category or service, the helpdesk can be notified in runtime about the decision taken. For example, the SLA rule engine may provide the message that "all Bronze subscribers for the free Poker Service are currently at reject status due to extremely high interest in the Platinum World Cup Soccer Service". This type of notifications will thus enable improved end-user support through the helpdesk.

While the invention has been described with reference to specific exemplary embodiments, the description is in general only intended to illustrate the inventive concept and should not be taken as limiting the scope of the invention. For example, the SIP signalling protocol and IMS concept have been used throughout when describing the above embodiments, although any other standards and service networks may basically be used. The present invention is defined by the appended claims.

CLAIMS

1. A method of controlling a service level agreement for a communication service in a mobile services access network (402), comprising the following steps:
- creating a network performance rule (400b) valid for said service level agreement and being based on an associated performance indicator (406) indicating the current network performance with respect to the fulfilment of said service level agreement,
- monitoring said performance indicator,
- evaluating said network performance rule based on the monitored performance indicator, and
- registering an agreement violation and/or taking measures to improve the network performance, if the evaluated network performance rule is not satisfied.

2. A method according to claim 1, wherein said measures to improve network performance includes modifying or adding a session admission rule applied for individual terminals and session requests, to introduce access constraints.

3. A method according to claim 2, wherein the session admission rule is used by a rule engine (410) of a policy unit to control the admission of individual sessions.

4. A method according to any of claims 1-3, wherein the network performance rule includes a degradation rule specifying a degradation level or limit of the monitored performance indicator, and a violation rule specifying a violation level or limit of the monitored performance indicator when the network performance has deteriorated

so that said service level agreement is deemed to be violated.

5. A method according to claim 4, wherein the degradation and violation rules are conditional by dictating said measures to improve network performance if the respective rule is not met.

6. A method according to claim 5, wherein the degradation rule is evaluated on a regular basis and the violation rule is evaluated if the degradation rule is not satisfied.

7. A method according to any of claims 4-6, wherein the service level agreement is deemed to be violated if the monitored performance indicator exceeds the violation level for more than a maximum acceptable time period.

8. A method according to any of claims 1-7, wherein the network performance rule is dependent on a plurality of associated performance indicators indicating different aspects of the current network performance with respect to the fulfilment of said service level agreement.

9. A method according to any of claims 1-8, wherein a Service Level Objective is defined based on one or more monitored performance indicators, such that the service level objective is deemed to be fulfilled as long as the associated performance indicators remain within acceptable limits.

10. A method according to any of claims 1-9, wherein said one or more monitored performance indicators relate to any of: bandwidth occupation, latency, packet loss rate, available bitrate, or network and service accessibility.

11. A method according to any of claims 1-10, wherein the monitored performance indicator is derived from a session database (408) used by the mobile network.

12. A service assurance module (400) in a mobile services access network (402) for controlling service level agreements for communication services, comprising:
- means for creating a network performance rule (400b) valid for a service level agreement and being based on an associated performance indicator (406) indicating the current network performance with respect to the fulfilment of said service level agreement,
- means for monitoring said performance indicator,
- means for evaluating said network performance rule based on the monitored performance indicator, and
- means for registering an agreement violation and/or for taking measures to improve the network performance, if the evaluated network performance rule is not satisfied.

13. A module according to claim 12, wherein said measures taking means is adapted to modify or add a session admission rule applied for individual terminals and session requests, to introduce access constraints.

14. A module according to claim 13, wherein the session admission rule is used by a rule engine (410) of a policy unit to control the admission of individual sessions.

15. A module according to any of claims 12-14, wherein the network performance rule includes a degradation rule specifying a degradation level or limit of the monitored performance indicator, and a violation rule specifying a violation level or limit of the monitored performance indicator when the network performance has deteriorated so that said service level agreement is deemed to be violated.

16. A module according to claim 15, wherein the degradation and violation rules are conditional by dictating said measures to improve network performance if the respective rule is not met.

17. A module according to claim 16, wherein the evaluating means is adapted to evaluate the degradation rule on a regular basis, and to evaluate the violation rule if the degradation rule is not satisfied.

18. A module according to any of claims 15-17, wherein the service level agreement is deemed to be violated if the monitored performance indicator exceeds the violation level for more than a maximum acceptable time period.

19. A module according to any of claims 12-18, wherein the network performance rule is dependent on a plurality of associated performance indicators indicating different aspects of the current network performance with respect to the fulfilment of said service level agreement.

20. A module according to any of claims 12-19, further comprising means for defining a Service Level Objective based on one or more monitored performance indicators, such that the service level objective is deemed to be fulfilled as long as the associated performance indicators remain within acceptable limits.

21. A module according to any of claims 12-20, wherein said one or more monitored performance indicators relate to any of: bandwidth occupation, latency, packet loss rate, available bitrate, or network and service accessibility.

22. A module according to any of claims 12-21, wherein the monitoring means is adapted to derive the performance indicator from a session database (408) used by the mobile network.

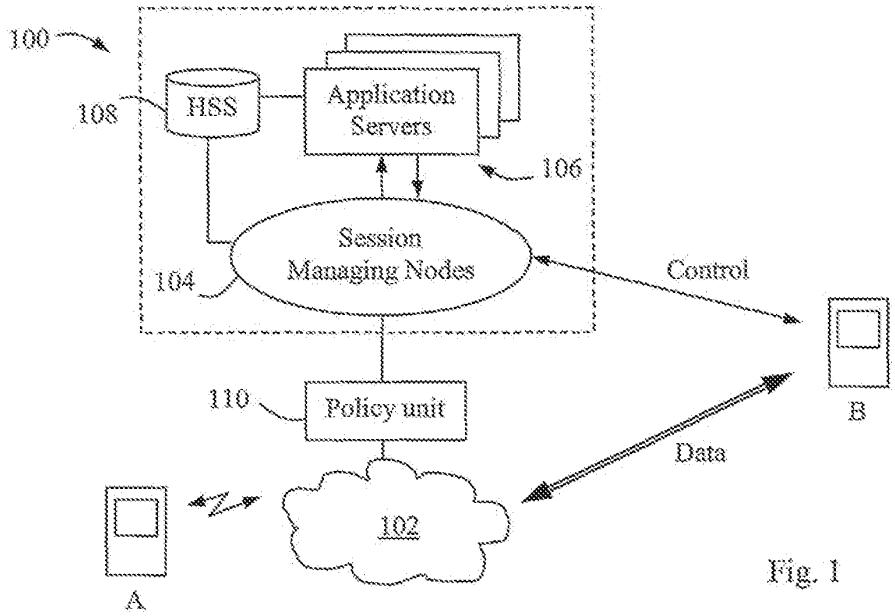

100
108
HSS
Application Servers
106
Session Managing Nodes
104
Control
110
Policy unit
B
Data
102
A

Fig. 1

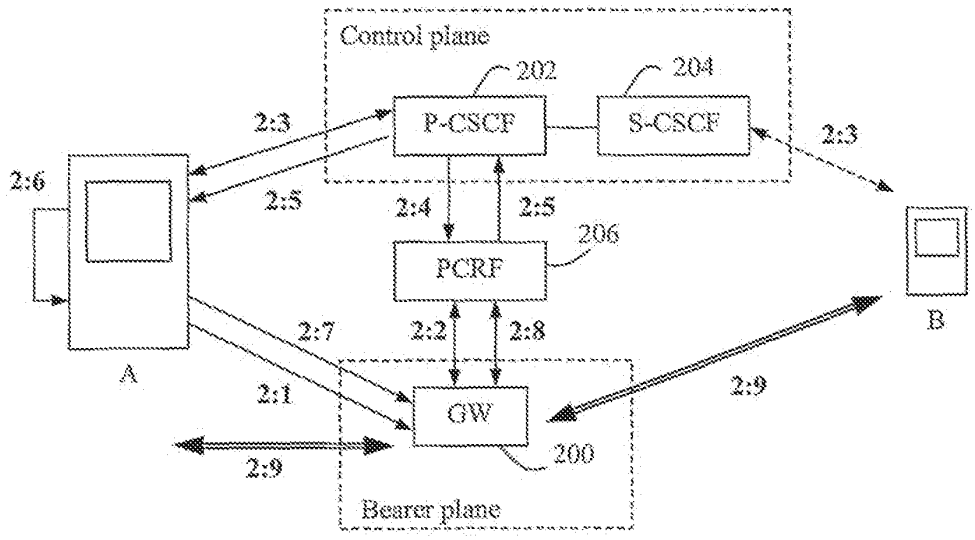

Control plane
202
204
P-CSCF
S-CSCF
2:3
2:3
2:6
2:5
2:4
2:5
206
PCRF
B
2:7
2:2
2:8
A
2:1
GW
2:9
2:9
200
Bearer plane

Fig. 2

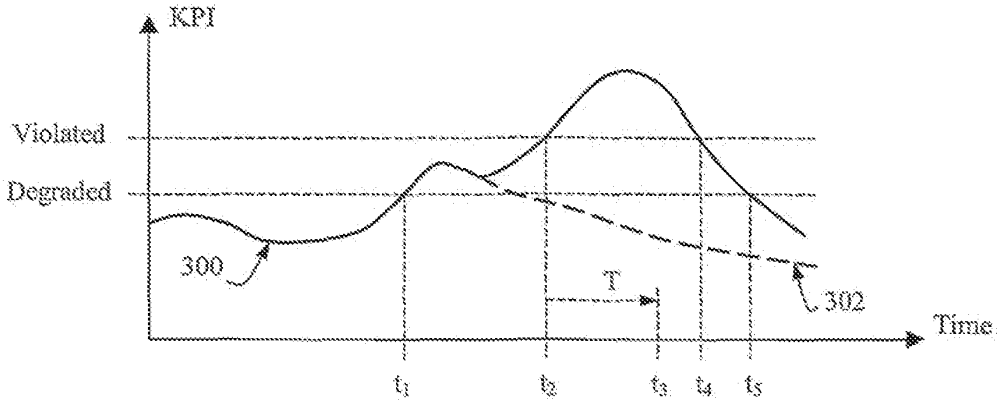

KPI
Violated
Degraded
300
T
302
Time
t1
t2
t3
t4
t5

Fig. 3

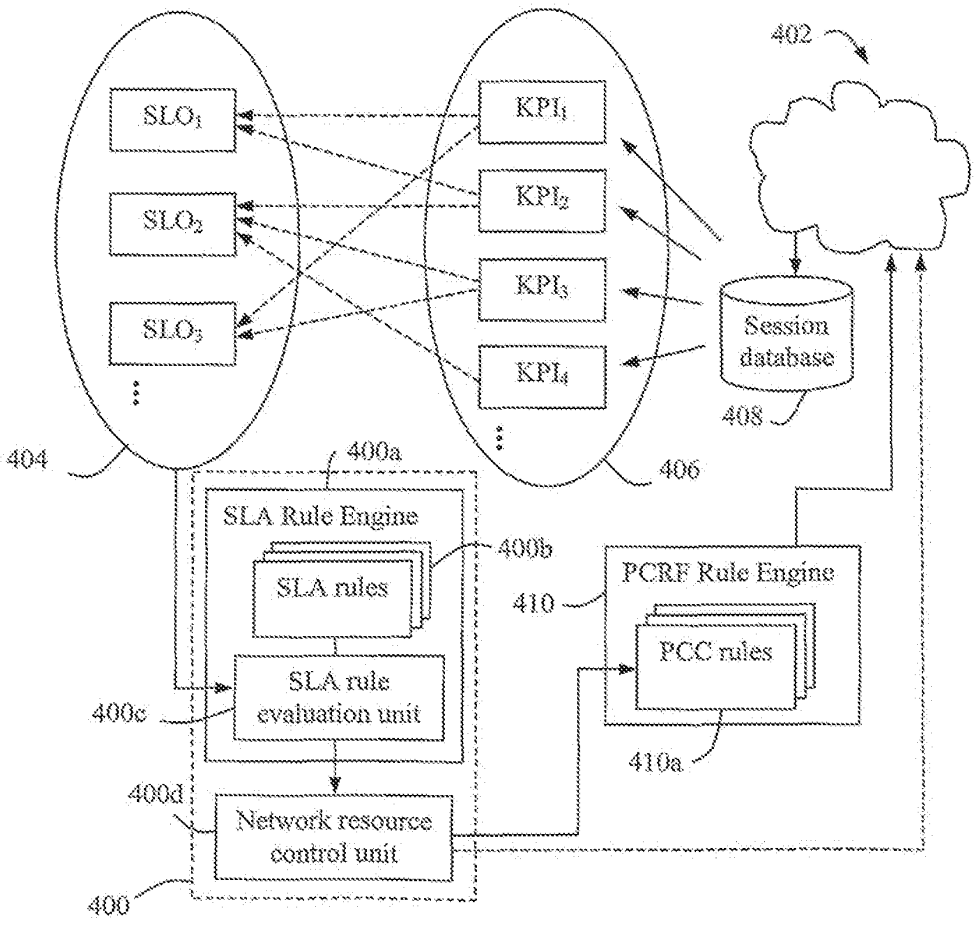

SLO1
SLO2
SLO3
KPI1
KPI2
KPI3
KPI4
402
Session database
408
404
406
400a
SLA Rule Engine
400b
SLA rules
SLA rule evaluation unit
400c
400d
Network resource control unit
400
PCRF Rule Engine
410
PCC rules
410a

Fig. 4

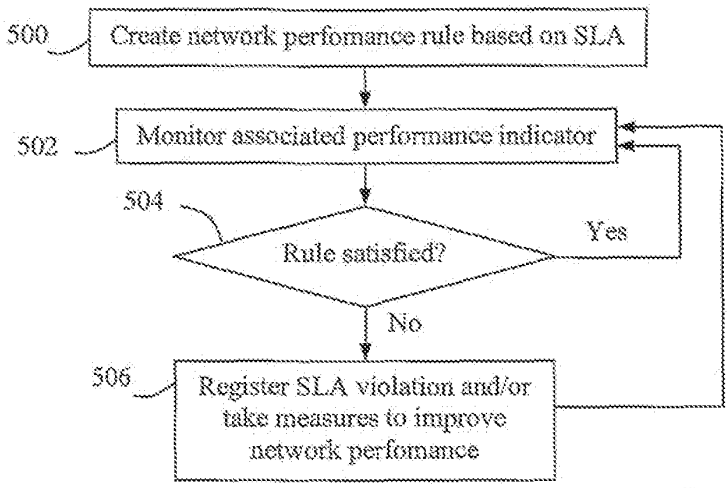

500
Create network performance rule based on SLA
502
Monitor associated performance indicator
504
Rule satisfied?
Yes
No
506
Register SLA violation and/or take measures to improve network performance

Fig. 5

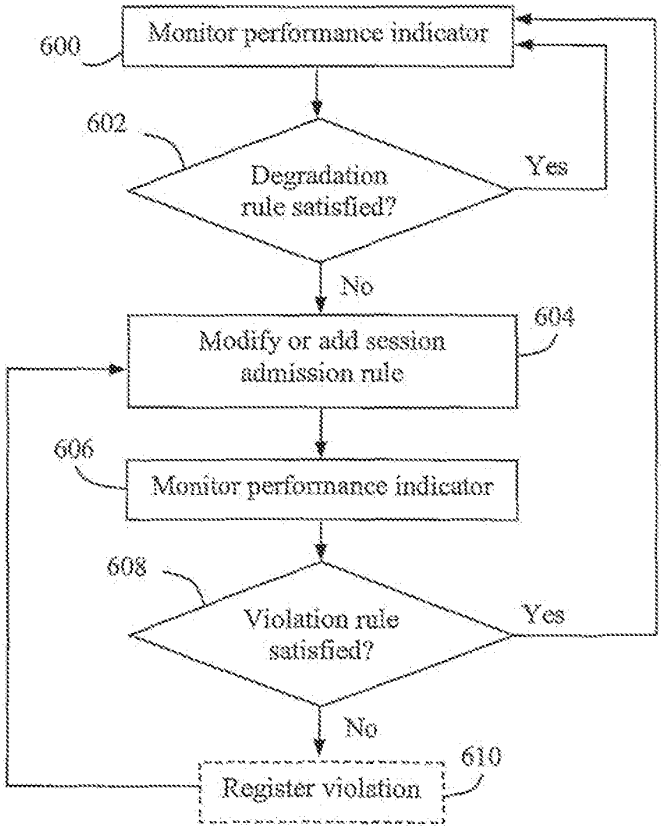

600
Monitor performance indicator
602
Degradation rule satisfied?
Yes
No
604
Modify or add session admission rule
606
Monitor performance indicator
608
Violation rule satisfied?
Yes
No
610
Register violation

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2006/001364

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04Q, H04L

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 0117169 A2 (ANDERSEN CONSULTING LLP), 8 March 2001 (08.03.2001), page 3, line 3 - line 14; page 38, line 9 - line 22; page 41, line 3 - line 28, page 47, line 2 - page 48, line 23; page 92, line 1 - page 95, line 11, claims 1-15, abstract --	1-22
A	WO 03084133 A1 (NETWORK GENOMICS INC), 9 October 2003 (09.10.2003), paragraphs 0002-0004; 0011-0017, claims 1-6, abstract --	1-22
A	EP 1259030 A2 (GATEWAY INC), 20 November 2002 (20.11.2002), paragraphs 0002-0009 -- --------	1-22

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2007	23 -07- 2007
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Elisabet Aselius/CM Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (April 2007)

International patent classification (IPC)
H04Q 3/00 (2006.01)
H04L 12/24 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.
The password is **EBVIQUCPIL**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

WO	0117169	A2	08/03/2001	AU	7109200 A	26/03/2001
				TW	226164 B	01/01/2005
WO	03084133	A1	09/10/2003	AU	2003228411 A	13/10/2003
				US	20040153563 A	05/08/2004
EP	1259030	A2	20/11/2002	JP	2002374303 A	26/12/2002
				US	20020174217 A	21/11/2002

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
18 May 2006 (18.05.2006)

(10) International Publication Number
WO 2006/050758 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number:
PCT/EP2005/002837

(22) International Filing Date: 17 March 2005 (17.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/626,691 10 November 2004 (10.11.2004) US

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BOMAN, Krister [SE/SE]; Nimbusgatan 3, S-431 44 Mölndal (SE).

(74) Agents: BERGENTALL, Annika et al.; Cegumark AB, P.O. Box 53047, S-400 14 Göteborg (SE).

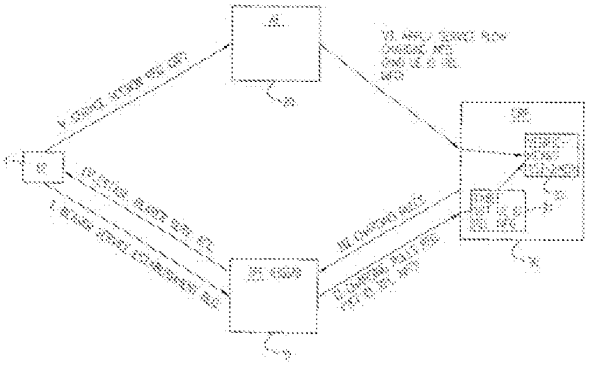
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,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

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

Published:
— *with international search report*

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

(54) Title: AN ARRANGEMENT, NODES AND A METHOD RELATING TO SERVICES ACCESS OVER A COMMUNICATION SYSTEM



(57) Abstract: The present invention relates to an arrangement in a communications system participating in user station (UE;1) service request and/or access procedures and comprising a number of packet data support nodes (10), a number of charging and/or policy handling nodes (30) and a number of application functions (20) handling mobility management and call control of mobile user stations requesting and/or accessing services. The packet data support node(s) (10) comprise(s) means adapted to send first mobile user station identity related information over a first interface (Gx,Gy;Gx/Gy) to a charging and/or policy handling node (30), at reception of a request for bearer services from a mobile user station (1). The application function(s) (20) comprise(s) means for, at reception of a request for a service session (SIP) from a mobile user station (1), sending second mobile user station identity related information to the charging and/or policy handling node (30), over a second interface (Rx,Rx/Gq). The policy and/or charging handling node (30) comprises verification means (32) adapted to establish whether the request for a bearer service to the packet data support node (10) and the request for a service session to the application function (20) (AF;P/S-CSCF) originate from one and the same mobile user station (1).

WO 2006/050758 A1

Title:

AN ARRANGEMENT, NODES AND A METHOD RELATING TO SERVICES ACCESS OVER A COMMUNICATION SYSTEM

FIELD OF THE INVENTION

The present invention relates to an arrangement in a communications system participating in user station service request or access procedures and it comprises a number of packet data support nodes, a number of charging and/or policy handling nodes and a number of application functions handling mobility management and call control of mobile user stations requesting or accessing services. The invention also relates to a node in a communications system supporting communication of packet data which is arranged to communicate with an application function and a packet data support node.

Still further the invention relates to a method involved in service request/access, in a communications system supporting communication of packet data and comprising a number of packet data nodes, a number of charging and/or policy handling nodes and a number of application functions handling mobility management and call control of mobile user stations requesting/accessing services.

STATE OF THE ART

So called IM (Internet IP Multimedia) services are getting more and more attractive and are already widely used. 3GPP IMS (IP Multimedia Subsystems) provides an IP-based session control

capability which is based on the SIP protocol (Session based Initiation Protocol). IMS may for example be used for the provisioning of services such as push-to-talk, instant messaging, presence and conferencing. IMS in UMTS (Universal Mobile Telecommunication System) will support IP multimedia applications such as video, audio and multimedia conferences. As referred to above, 3GPP will use the SIP, Session Initiation Protocol, as the signalling protocol for creating and terminating multimedia sessions, c.f. for example IETF RFC (Request For Comments) 3261, which deals with how the SIP signalling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS.

The current security architecture for IMS is specified in 3GPP TS 33.203. However, it is a problem that implementations of the services referred to above will exist which are not fully compliant with 3GPP IMS. 3GPP IMS for example exclusively uses IPv6 (Internet Protocol version 6) although there may still be IMS implementations based on IPv4. However, the use of IPv4 instead of IPv6 is only one of the differences between "early" IMS implementations and implementations complying with 3GPP IMS to a full extent. It has been recognized that non-compliance with 3GPP TS 33.203 security features, will mainly produce problems at the user equipment (UE) due to the potential lack of support of the USIM/ISIM interface, particularly for user stations only complying with 2G. It has therefore been realized that, for such "early" IMS implementations, mechanisms are needed to protect against the most significant security threats.

Such a temporary solution for "early" IMS implementations is suggested in 3GPP TR 33.878. The approach in this document is that the GGSN (Gateway GPRS Support Node) shall send MSISDN and

the IP address of a user station (User Equipment UE) towards a Radius server over the Gi interface. The Radius server then forwards the MSISDN and IP address to the HSS (Home Subscriber Server). When the user station, or the UE, sends a SIP register request towards a Serving-Call/Session Control Function (S-CSCF), including the IM (IP Multimedia) private identity, the S-CSCF will query the HSS, which, based on the IMS identity can identify the matching MSISDN and IP address of the UE and return the IP address to the S-CSCF. The S-CSCF will check with the stored IP address in the S-CSCF to see if it matches the received IP address from the UE. If the two IP addresses are the same, the S-CSCF can proceed with the registration procedure but if they are not the same, presumably due to an attack being in progress, the session is terminated. This gives a possibility to avoid certain attacks such as for example an attacker using the IMS identities of a victim, which may have as a consequence that the attacked user has to pay for the service accessed by the attacker.

An operator also runs the risk that the attacker does not pay for the bearer, e.g. a conversational bearer, due to the fact that for example FBC (Flow Based Charging) is implemented and zero rates the bearer. This means that for some use cases, an attacker could use certain services for free.

3GPP TR 33.878 assumes that "During a PDP-context request towards the IMS, the GGSN shall send a "Radius Accounting-Request-Start" message to a Radius server attached to the HSS. This may lead to the assumption that an operator uses a specific IMS APN (Access Point Name) or that the UE uses a signalling PDP-context. It is however believed that the assumption relating to the use of a specific IMS APN is too restrictive from an architectural point of view. 3GPP TS 23.228 stipulates that

"When the UE uses GPRS-access for IMS services, it shall be able to establish a dedicated signalling PDP-context for IM subsystem related signalling or utilize a general-purpose PDP-context for IM subsystem signalling traffic". There is hence no guarantee that the UE uses a signalling PDP-context for IMS, may lead to the conclusion that the GGSN should then send the IP address of a UE towards a Radius server for all services. Further, an UE may have several IP addresses towards one and the same GGSN and it appears necessary that the GGSN, in such a case, has to send all these IP addresses towards the Radius server. Furthermore, in the general case a UE may be attached to more than one GGSNs or it may have activated more than one IP network connections. Such scenarios are not discussed in 3GPP TR 33.878.

Furthermore, the solution discussed in this document suggests the introduction of a so called "idle timer" in GGSN. This has an impact on how IP addresses towards an UE are allocated or released and an IP address can be reused for a user when re-establishing a PDP-context at a later stage. Apparently the reason for the introduction of the idle timer is to reduce the load on the HSS and, when there is no PDP-context available between GGSN and an UE, the GGSN stores or reserves the allocated IP address for a specific UE for a time which is equal to the time period set in the idle timer. This means that the GGSN does not upon termination of all bearers send an accounting-request stop until the idle timer has expired. Thus the idle timer has not been introduced for security reasons but in order to reduce the communication towards the HSS which is responsible for the creation of authentication vectors and hence the intention is to reduce communication with the HSS, or not to allow more communication with HSS than necessary in order to avoid that it becomes overloaded, which might have the effect that other services, for example voice, would suffer. The use of

the idle timer is disadvantageous for example in that there will be an increasing risk for conflicts between dynamically allocated IP addresses. Furthermore resources are held more than necessary.

The suggested solution is also disadvantageous in that more and more information is sent from GGSN over the Gi interface which will become more and more loaded. It is also disadvantageous that a Radius server is needed in order to verify the IP addresses and, as referred to above, it does not take general architectures into account such as when a UE for example is attached to more than one GGSN and/or has activated more than one IP network connection etc.

SUMMARY OF THE INVENTION

Therefore an arrangement as initially referred to is needed through which IMS security can be provided for in a straight-forward and easy manner. Particularly an arrangement is needed through which so called "early" IMS security can be provided, i.e. in networks still not (fully) complying with the 3GPP TS 33.203 Release 5. Particularly an arrangement is needed through which attacks can be detected and prevented and particularly through which security can be increased for end users as well as for operators, for example such that an attacker is prevented from using certain services for free or making someone else pay for it, and that an attack can be detected as early as possible which is extremely important for the end user as well as for the operator.

Particularly an arrangement is needed which is flexible and which can be adapted to different network environments, such as for example so called aware network environments. Still further an arrangement is needed which takes into account and takes

advantage of the development for example within 3GPP or similar systems. Still further an arrangement is needed through which the amount of information sent over the so called Gi interface from Gateway GPRS Support Nodes or similar can be reduced instead of increased. Most particularly an arrangement is needed through which there is no need for the introduction of additional nodes and more generally through which the number of nodes involved and affected can be kept as low as possible. An arrangement is also needed which reduces or even eliminates the drawbacks and impacts on IP address allocation or release towards an UE arising through the introduction of a so called idle timer in a GGSN.

Still further an arrangement is needed which can be used in a general architecture and which takes into account situations, as for example when a user equipment is attached to more than one GGSN (or CGSNs or other gateways) and/or when a user equipment has activated more than one IP network connection. Still further a node is needed which assists in provisioning of one or more of the objects referred to above. Still further a method is needed through which one or more of the abovementioned objects can be achieved.

Therefore an arrangement as initially referred to is provided wherein the packet data support node(s)/comprise(s) means adapted to send first mobile user station identity related information over a first interface (Gx,Gy;Gx/Gy) to a charging and/or policy handling node, at reception of a request for bearer services from a mobile user station, the application function(s) comprise(s) means for, at reception of a request for a service session (SIP) from a mobile user station (UE), sending second mobile user station identity related information to the charging and/or policy handling node, over a second interface (Rx,Rx/Gq), and wherein the

policy and/or charging handling node comprises verification means adapted to establish whether the request for a bearer service to the packet data support node and the request for a service session to the application function (AF;P/S/I-CSCF) originate from one and the same mobile user station (UE). Particularly the first mobile user station identity related information comprises one or more of MSISDN, IMSI and IP address of the mobile user station, and the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU), or IMSI and/or MSISDN, e.g. derived from IMS private or public identity (IMPI,IMPU), or the application function being adapted to fetch said information externally, e.g. from a HSS.

Particularly the IP addresses are received in, or derived from, the first mobile user station related information and the second mobile user station identity related information, and the verification means are adapted to compare the IP address obtained from the application function (AF) with the IP address obtained from the packet data support node. In one embodiment the verification means are adapted to, if required, establish and, use IMSI and/or MSISDN of said first and second mobile user station identity related information respectively, to compare the associated IP addresses. The charging and/or policy handling node may also be adapted to deduce IMSI and/or MSISDN from a received IMS private and/or public user identity (IMPI/IMPU).

In an advantageous embodiment the charging and/or policy handling node is adapted to construe a private user identity using IMSI of a mobile user station, e.g. when no ISIM application is implemented and further it is particularly adapted to identify and install charging rules to be applied at reception of a request therefor from a packet data support node.

According to the invention, if the first and second user identity related information do originate from one and the same mobile user station, the charging and/or policy handling node is particularly adapted to implement the provisioned charging rules. If, on the other hand, the first and second user identity related information do not originate from one and the same mobile user station, the charging and/or policy handling node may be adapted to reject the charging rules and/or deactivate implemented charging rules and discard concerned IP flow traffic, and further be adapted to inform the application function (AF) that no PDP-context is available.

Alternatively, if the first and second user identity related information do not originate from one and the same mobile user station, the charging and/or policy handling node may be adapted to select whether to or deactivate the charging rules in the packet data support node, or to keep them active (or activate them). In a particular embodiment the packet data support node comprises a node handling Traffic Plane Functions (TPF), e.g. a GGSN implementing TPF or a CGSN implementing TPF. It may alternatively comprise a stand-alone node or a gateway node handling TPF or TPF and policy enforcement (PEP).

According to different embodiments the charging and/or policy handling node comprises a CRF, a PDF or a PCCN. Particularly the first interface is Gx or Go/Gx merged with Gy if the charging and/or policy handling node is merged with an OCS, and the second interface comprises Rx or Rx merged with Gq.

A node (functional, logical or physical) in a communication system as initially referred to is also provided which is adapted to receive first mobile user station identity related information from a packet data support node relating to a bearer service

request for a mobile user station, or at reception of a request for a bearer service from a mobile user station (UE) in the packet data support node, to receive second mobile user station identity related information from an application function relating to a service session or at reception of a request for a service session therein, and comprises verification means for establishing whether the request for a bearer service (to the packet data support node) and the request for a service session (to the application function) originate from the same mobile user station. Particularly the first mobile user station identity related information comprises one or more of MSISDN, IMSI and IP address of the mobile user station. Even more particularly the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU) of the mobile user station or IMSI and/or the handling node is adapted to derive IMSI and/or MSISDN from IMPI and/or IMPU and/or adapted to request said IMSI and/or MSISDN from the application function.

The verification means are preferably adapted to compare the IP address corresponding to or included in the first mobile user station identity related information and the IP address corresponding to or included in the second mobile user station identity related information, and particularly to, if required establish and, use IMSI and/or MSISDN of said first and second mobile user station identity related information, to compare the associated IP addresses. Alternatively it is adapted to derive IMSI and/or MSISDN from a received IMS private and/or public user identity (IMPI/IMPU). Particularly the charging and/or policy handling node is adapted to construe a private user identity using IMSI of a mobile user station, e.g. when no IMSI application is implemented.

It may also be adapted to identify and install charging rules to be applied at reception of a request therefor from a packet data support node. Particularly it is adapted to identify and install charging rules to be applied at reception of request therefor from a packet data support node, and if the first and second user identity related information do originate from one and the same mobile user station, to implement the provisioned charging rules, and, if the first and second user identity related information do not originate from one and the same mobile user station, to reject the charging rules and/or deactivate implemented charging rules and discard concerned IP flow traffic, to inform the application function (AF) that no PDP-context is available or, to select whether to deactivate the charging rules in the packet data support node, or keep them active, if activated. Particularly it comprises a CRF, a PDF or a PCCN or a node with a similar functionality.

Still further a method as initially referred to is provided which comprises the steps of; receiving a request for bearer services from a mobile user station in a packet data support node; sending, from the packet data support node, first mobile user station identity related information of the mobile user station to a charging and/or policy handling node; receiving, subsequently, before or substantially simultaneously, a request for a service session from the mobile user station in an application function; sending, from the application function, second mobile user station identity related information to the charging and/or policy handling node; establishing, in the charging and/or policy handling node, whether the request for a bearer service to the packet data support node and the request for a service session to the application function originate from the same mobile user station.

As referred to earlier, particularly the first mobile user station identity related information comprises one or more of the MSISDN, IMSI and IP address of the mobile user station, and the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU), or the second user identity related information comprises IMSI and/or MSISDN, e.g. derived from IMS private or public identity (IMPI,IMPU), or the application function is adapted to fetch said information from a HSS. Particularly the method further comprises the steps of; establishing or finding IMSI and/or MSISDN of said first and second mobile user station identity related information, comparing at least part of said first and said second mobile user station identity related information with each other, and even more particularly of comparing the IP addresses of said first and second mobile user station identity related information and/or deriving IMSI and/or MSISDN from received IMS private and/or public user identities (IMPI/IMPU), and/or construing, in the charging and/or policy handling node, a private user identity using IMSI of the mobile user station, e.g. when no ISIM application is implemented.

Advantageously it also comprises the step of; identifying and installing applicable charging and/or policy rules at reception of a request from a packet data support node. Most particularly the method further comprises the steps of; if the first and second mobile user station identity related information do originate from one and the same mobile user station; implementing the provisioned applicable charging rules and/or policy rules in the charging and/or policy handling node, otherwise, discarding concerned IP flow traffic; or selecting whether to keep active or deactivate the charging rules. In preferred implementations the packet data support node comprises a node handling Traffic Plane Functions, and is a stand-alone node, or a GGSN or a CGSN or a gateway node

handling TPF and policy enforcement (PEP), and the charging and/or policy handling node comprises a CRF, a PDF or a PCCN or a node with a similar functionality.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will in the following be further described, in a non-limiting manner, and with reference to the accompanying drawings in which:

Fig. 1 shows a "state of the art" solution,

Fig. 2 is a schematical block diagram illustrating an arrangement according to the present invention,

Fig. 3 is a simplified sequence diagram illustrating the provisioning of the first mobile user station identity related information to a charging and/or policy handling node,

Fig. 4 is a simplified sequence diagram including the procedure when the second mobile user station identity related information is provided to the charging and/or policy handling node,

Fig. 5 is a sequence diagram illustrating an exemplary procedure of the provisioning of the second mobile user station identity related information and verification thereof,

Fig. 6A is a sequence diagram describing an exemplary implementation and wherein the verification result is positive,

Fig. 6B is a sequence diagram describing the exemplary implementation of Fig. 6A but wherein the verification result is negative,

Fig. 7 is a schematical block diagram illustrating the inventive concept implemented in one general architecture,

Fig. 8A illustrates another general architecture in which the inventive concept can be implemented,

Fig. 8B shows still another architecture in which the inventive concept can be implemented, and

Fig. 9 is a flow diagram describing the procedure according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 shows the state of the art solution discussed earlier in the application for providing security for IMS accesses, particularly for early implementations of IMS not yet complying with the requirements of 3GPP TS 33.203. Such a solution is among others discussed in 3GPP TR 33.878. It is supposed that an UE 1_0 requests a bearer from GGSN 10_0. PDP-contexts are set-up in a conventional manner, primary or secondary depending on which is the relevant procedure. The user equipment UE 1_0 may have several IP addresses, one IP address per IP network connection. GGSN comprises an idle timer 11_0 through use of which an IP address can be reused for a user when re-establishing a PDP-context at a later stage. There is no specific IMS APN (Access Point Name) and GGSN cannot assume use of a signalling PDP-context. Knowing, in a conventional manner MSISDN and the IP address of UE 1_0, GGSN 10_0 sends MSISDN and the IP addresses over

the Gi interface towards Radius Server 30_0, i.e. all UE IP addresses and MSISDN are sent. The idle timer used in GGSN 10_0 apparently is intended mainly to reduce the load on the HSS. This is suggested to be in the order of hours working in such a way that when there is no PDP-context available between GGSN and UE, the GGSN stores or reserves the allocated IP address for a specific UE for a time period which corresponds to the time set in the idle timer. This would mean that the GGSN does not upon termination of all bearers send any accounting-request-stop until the idle timer has actually expired. This idle timer does influence how IP addresses towards the UE are allocated or released.

The Radius Server 30_0 forwards the information, i.e. MSISDN and the IP address to HSS 40_0. All UE IP addresses and the MSISDN are sent according to the idle timer 11_0 in the GGSN 10_0, i.e. the sending will generally be slowed down, or delayed, until the idle timer expires.

Then a request for a SIP registration (SIP REGISTER) is sent from UE 1_0 to S-CSCF, the S-CSCF sends the IMS identity onto the HSS 40_0. HSS 40_0 returns a reply to S-CSCF with the registered IP address back to the S-CSCF 20_0. S-CSCF 20_0 comprises a verification means 21_0 or a functionality for performing a verification through verifying that the IP address from HSS 40_0 is the same as the stored IP address in S-CSCF. If they are not the same, the session is terminated because it is assumed that an attack is ongoing.

The disadvantages of such a solution has been discussed earlier in the application.

Fig. 2 shows an arrangement according to one implementation of the inventive concept according which a FBC (Flow Based Charging) architecture is reused. The problem that is solved through the arrangement consists in the provisioning of a mechanism ensuring that the network is enabled to verify that the IP address of a user equipment UE 1 and the IMS identity of the UE 1 at SIP layer correspond to the same user at the bearer level. According to invention, the involved nodes or functions are the GGSN 10 handling traffic plane function TPF, (according to the inventive concept it is the traffic plane function that is used and it may be realized as a stand-alone node, provided in a GGSN or in a CGSN or in any node at least including the TPF functionality), a charging and/or a policy handling node 30 which in this embodiment is implemented as a CRF (Charging Rules Functionality) and an application function AF 20 which may be implemented as a S-CSCF, a P-CSCF or similar, and the concerned user equipment UE 1. CRF 30 comprises storing means, e.g. a table for storing first user equipment identity related information as will be explained below, and verification means 32 for verifying if at least a given part of a first UE identity related information corresponds to second UE identity related information, e.g. through comparing at least parts of said first and second identity related information respectively. By at least part of is meant that it might not be necessary to compare all the information depending on implementations, as also will be explained below. It is, however, in Fig. 2 supposed that UE 1 sends a request for bearer service establishment (I) to TPF 10 which may be implemented in a GGSN. TPF 10 then, in for example a CRF based implementation, as in Fig. 2, requests for charging rules (II) from CRF 30. First UE identity related information accompanies the request. The first UE identity related information may be provided from the UE or provided from TPF 10 (if it for example relates to a secondary PDP-context request).

How this is done or acquired is not of importance for the functioning of the present invention, the main thing being that the first UE identity related information is available in TPF 10. The first UE identity related information accompanying the charging rules request is then stored into table 31 in CRF 30, CRF 30 among others using the first UE identity related information and possibly other information, for example QoS information about application function etc., identifies which are the relevant charging rules to be installed, and then provides the charging rules to TPF 10 (III). TPF 10 performs the relevant charging rule actions or provides for implementation of the provisioned charging rules, and sends an acceptance message relating to the establishment of the bearer service request, (IV) to UE 1.

Once a bearer has been established, UE 1 sends a request for a service session using SIP, (V) to AF 20. In GPRS systems, and from an FBC point of view, a proxy-CFCS and/or a serving-CFCS and/or an Interogating CSCF may, depending on operator configuration, act as an AF operating the Rx interface and/or the Gq interface. In the request using the SIP protocol, second user identity related information of the requesting is included. AF 20 then sends application/service flow charging information, including the second UE identity related information to CRF 30 (VI). If for example an S-CSCF acts as an AF, it may, before a registration session is proceeded, unsolicited forward the private user identity along with the IP address of the UE over Rx towards CRF 30. At PDP-context activation, FBC assumes that the IP address of the UE and IMSI (or MSISDN) are sent towards the CRF 30 over the Gx interface. Based on the above assumptions, CRF 30 is then aware of the IMSI both from the AF 20, particularly S-CSCF, and the TPF 10, particularly GGSN, and the corresponding IP addresses and hence capable to, in the

verification means 32, check if the IP addresses match or originate from one and the same user (in Fig. 1 they actually both originate from the same UE, namely UE 1). If they do not correspond, or do not originate from one and the same end user, i.e. if there is no match between the IP addresses, CRF 30 (in this case; it should be clear that for policy handling the node could be a PDF, but it may also be a PCCN for handling policy and/or charging) notifies the AF 20, particularly S-CSCF, in order to provide for a termination of the SIP session, and the CRF 30 should deactivate any corresponding rule(s) at the TPF 10.

It could of course also be optional whether the session should be terminated or not and optionally it may be operator controlled, such that under certain circumstances for example an operator might want to localize or track an attacker and therefore would let the session proceed. Also for other reasons an operator might allow the session under certain conditions etc. The invention is not limited to any particular measures to be taken, but it is fundamental that an awareness is provided concerning the correspondence of addresses and possible attacks or similar.

The second user identity related information sent from AF 20 to CRF 30 may for example contain IMPI (IMS Private Identity), IMPU (IMS Public Identity), and the IP address. Alternatively the AF 20 may send IMSI or MSISDN directly. This can either be derived from the private identity or alternatively the AF, e.g. S-CSCF may contact HSS to identify IMSI or MSISDN.

If for example the UE does not contain an ISIM, (but for example an USIM) IMPI may be derived and the private user identity

should take the form of a NAI and shall have the form username@realm as specified in IETF RFC 2486, clause 3.

A representation of the IMSI may be contained within the NAI for the private identity.

If there is no ISIM application, the private user identity is not known and it may then be derived from IMSI. The private user identity may be construed out of the IMSI by using the whole string of digits as username part of the private user identity, and by converting the leading digits of the IMSI, i.e. MNC and MCC into a domain name.

The result will be a private user identity of the form: "<IMSI>@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org". For example: If the IMSI is 234150999999999 (MCC=234, MNC=15), the private user identity will takes the form 234150999999999@ims.mnc015.mcc234.3gppnetwork.org

Hence, CRF/PDF (PCCN) is capable to, based upon the reception of IMPI, i.e. the IMS Private Identity, or even IMPU, the Public User Identity, and IP address from an AF, for example a CSCF such as P-CSCF, S-CSCF, or I-CSCF, over Rx or Gq or Rx merged with Gq, derive IMSI (or MSISDN) of the UE. It should be noted that the AF alternatively may send MSISDN and/or IMSI directly over Rx/Gq as referred to above.

Furthermore, since the TPF, here TPF implemented in a GGSN, shall have the capability to send the IMSI or MSISDN to the CRF/PDF/PFCN (over Gx or Gx/Gy if merged), the CRF/PDF can then match the IMSI (or MSISDN) from CRF and TPF (here GGSN) with the respective IP addresses, i.e., CRF 30 is capable to find IMSI (MSISDN) from, here, GGSN and AF and check that it is the same

IP address associated. If there is a match, the CRF preferably implements, in this case, charging rules as specified in 3GPP TS 23.125. If, on the other hand, the IP addresses do not originate from one and the same UE, the CRF may decide not to implement the charging rules or deactivate already implemented charging rules as referred to above, and hence the traffic may be discarded for the concerned IP flow. The CRF then informs the AF, e.g. a P-CSCF/S-CSCF that no PDP context is available.

Alternatively, may, in certain situations, as also referred to above, an operator want to allow the traffic, for example in order to track an attacker. Hence it may be an option for the charging and/or policy handling node 30 to keep rules in the TPF 10 active or to deactivate them.

In some implementations the TPF is implemented in a GGSN (or CGSN) but, as referred to above, TPF may be implemented in a stand-alone node or function or be allocated elsewhere than in a GGSN/CGSN, the main thing being that it is the traffic plane function TPF that is involved according to the inventive concept, since it is TPF that operates Gx towards CRF/PDF (or PCCN) (or Gx/Gy when merged).

The invention functions in a similar way for public user identities as for private user identities. 3GPP TS 23.003 specifies that when no ISIM is used, the temporary public user identity should be of the form "user@domain", and should therefore be equal to the private user identity. It is further possible to use a public user identity rather than the private identity at SIP layer. Then the AF, e.g. S-CSCF, may e.g. request an IMSI from HSS based on the public user identity, derive IMSI from the public user identity or send the public user identity towards CRF/PDF/PCCN that derives IMSI or sends a

query to a Subscription Profile Repository, if implemented, cf. Fig. 5, for getting IMSI or MSISDN.

Fig. 3 is a schematical sequence diagram illustrating the messaging between an UE, a TPF and, in this case a CRF. It should be clear, as referred to above, that the TPF can be provided for as a stand-alone node, in a GGSN, in a CGSN or in any other node or functioning means at least providing the TPF functionality. It should also be clear that instead of a CRF handling charging rules, it could as well be a PDF handling policy rules or a combined node or functionality handling e.g. both policy and charging. Hence, it is supposed that the UE, in a conventional manner, sends a request for establishment of a bearer service, 1, to e.g. a GGSN providing the TPF functionality. At PDP-context activation, first or primary, the GGSN, in this case, will send terminal identities such as one or more of IP address, MSISDN and IMSI towards CRF over the Gx interface in a request for charging rules, 2, i.e. the first user equipment identity related information is accompanying the request for charging rules. CRF stores the received first UE identity related information, 3, and identifies which are the charging rules that are applicable and should be installed, 4. Subsequently the charging rules are provisioned to TPF, 5. TPF at reception of the charging rules performs the charging rule action or actions, 6, and sends an establish bearer service acceptance message to UE, 7.

It should be clear that, as referred to above, the CRF may be merged with a PDF. Even more particularly CRF (and/or PDF or PCCN) may be merged with an Online Charging System OCS in which case Gx may be merged with Gy. These interfaces are defined in TS 23.125, and may e.g. in one embodiment both be based on Diameter Credit Control.

Fig. 4 is schematical sequence diagram illustrating the procedure through which the second UE identity related information is provided to CRF (for example) such that a verification can be carried out according to the inventive concept.

Hence, it is supposed that when UE sends a request for a service session using the SIP protocol, 8, to AF which e.g. may comprise a P-CSCF or an S-CSCF or an I-CSCF acting as an AF, this includes sending user identities to the CRF over Rx, which is described in 3GPP TS 23.228, which herewith is incorporated herein by reference. In other words, the UE sets up a SIP Register towards the IMS network. Hence, when a request for service session, SIP Register, 8, is sent to AF, AF provides application/service data flow charging information including second UE identity related information, e.g. IMPI, IMPU, IP address, to CRF, 9. CRF, having stored the first UE identity related information in storing means, fetches said first UE identity related information and compares it with the second UE identity related information received from the AF, 10. It is here supposed that the first and the second UE identity related information respectively originates from one and the same UE, and hence an acknowledgment, 11, is sent to AF and the service is setup implementing the relevant charging rules or similar.

It should be clear that the Rx interface may be merged with Gq and the AF may hence operate Rx/Gq. Rx and Gq may in particular embodiments both be based on Diameter Nasreq.

It should be clear that, as an alternative of sending IMPI and IMPU i.e. IMS private and public identity respectively as described in TS 23.228 and TS 23.003, the AF, or any CSCF, may

send IMSI or MSISDN directly to CRF. IMSI or MSISDN may be derived from the private identity or communication with HSS may be needed for identification of IMSI or MSISDN. This has been discussed earlier with reference to Fig. 2.

The CRF particularly comprises a table for translation between IMPI and IMSI.

Fig. 5 is a sequence diagram illustrating the procedure when the second UE identity related information is provided to e.g. a CRF or a PCCN etc., where (here) a successful verification is performed. It is here supposed that a PDP-context is established, and that the first UE identity related information is available in a CRF, PCCN etc. It is supposed that the UE is in a visited network and sends a SIP register, 80, with public user ID, private user ID, UE IP address to P-CSCF. The SIP register is sent from P-CSCF to I-CSCF of the UE home network, 81. I-CSCF sends a Diameter (in this particular embodiment) Cx-Query/Cx-Select-Pull message, 82, to HSS, which returns the corresponding response, 83, concerning IMS identities. SIP register with Public User ID, Private User ID, UE IP Address is then sent from I-CSCF to S-CSCF, 84. In this particular embodiment it is supposed that S-CSCF act as an AF. In alternative embodiments P-CSCF or I-CSCF may acts as AF. It shall be clear that here TPF and the subscription information repository are not visible.

Steps 85,86 relate to provisioning of security parameters, application IP address etc. which however is not of relevance for the inventive concept.

Subsequently it is supposed that the second UE identity related information, Public User ID, Private User ID, UE IP Address are

provided to CRF (PCCN etc.), 87, and after verification (here supposed to be affirmative) with the first UE identity related information (not shown here), an acknowledgement is sent to S-CSCF, 88. S-CSCF sends a positive verification message, 2XX OK to I-CSCF, 89, which forwards it to P-CSCF, 90, which in turn forwards it to UE, 91.

Fig. 6A shows one example of an implementation in which it is supposed that the 1st and 2nd UE identity related information can be positively verified (i.e. there is correspondence) and in which the Diameter protocol is used.

Thus, first the UE sends (here) an Activate PDP Context Request to (here) an SGSN, 1_1. In a conventional manner SGSN sends a Create PDP Context Request to GGSN, 2_1, which here uses a Radius Client to obtain IP addresses of UEs.

In this embodiment it is supposed that the Diameter protocol is used (cf. 3GPP TS 29.210), and GGSN sends a request for rules, here a Diameter CCR (Credit Control Request) with IMSI, MSISDN IP Address, over Gx to CRF (or PCCN etc.), 3_1. CRF responds with a Diameter CCA (Credit Control Answer) with charging rules over Gx, 4_1, to GGSN, which sends a Create PDP Context response to SGSN, 5_1. SGSN sends an Activate PDP Context Accept to UE, 6_1, with the allocated PDP Address (IP Address). As described earlier, it is supposed that the UE sends a SIP register to GGSN, 7_1, which checks for IP address spoofing (i.e. checks that the UE has not changed, i.e. uses another, IP address than the one it has been given). When it is verified that the UE uses the "correct" IP address, a SIP register is sent to P-CSCF, 8_1, which sends it to I-CSCF, 9_1. I-CSCF then sends the SIP register to C-CSCF (here acting as AF), 10_1.

In this embodiment it is supposed that S-CSCF sends a Diameter Message (Nasreg application) AAR to CRF, 11_1, over Rx and containing the public user ID of the UE, and the private user ID and the IP address of the UE. CRF maps private and/or public user identity to MSISDN and/or IMSI to retrieve the associated IP address. CRF then performs the verification, i.e. checks whether the information received from GGSN (cf. step 3_1) is the same, and acknowledges that the verification was successful (in this case) over Rx to S-CSCF in an AAA answer, 12_1.

Finally a SIP 2XX OK message is sent from S-CSCF to UE, 13_1.

Fig. 6B is similar to Fig. 6A with the difference that the mapping in CRF is unsuccessful. Hence steps 1_1-11_1 are similar to steps 1_1-11_1 in Fig. 6A and therefore bear the same reference numerals.

Upon establishing in CRF that the mapping is unsuccessful, i.e. that the first and second UE identity related information is not the same, an error message is sent over Rx (Diameter) to S-CSCF, 12_2. Optionally CRF may then send a Diameter CCA message over Gx to GGSN, 13_2, that the relevant charging rules should be removed. GGSN then confirms the removal to CRF, 14_2, and (in any case, irrespectively of whether steps 13_2, 14_2 are implemented or not) an error message is sent from S-CSCF to UE, e.g. a SIP 4XX Forbidden, 15_2.

It should be clear that the inventive concept is not restricted to the use of Diameter. Radius may also be used or any other appropriate protocol. As referred to above, the flow will also be different if a CGGN is used, instead of a GGSN and a SGSN which however is not explicitly illustrated since the alterations should be obvious.

As also referred to above, it does not have to be S-CSCF that acts as an AF, and instead of a CRF it may e.g. be a PDF, PCCN etc.

Fig. 7 shows a particular embodiment in which the charging and/or policy handling node comprises a PCCN 30A (Policy and Charging Control Node). PCCN 30A communicates with service data flow based credit control 36A or more generally OCS. If for example PCCN 30A receives an IMS identity, e.g. IMPI from an AF (not shown) it may request IMSI from the subscription profile repository 35 over the Sp reference point (or particularly Sp-interface). More generally, if PCCN 30A receives an IMS identity, it may query subscription profile repository 35 in order to get a connection between the IMS identity (IMPI or IMPU) and the MSISDN or IMSI received from the TPF, e.g. in GGSN. This is advantageous in that it also covers cases when users utilize an ISIM which may have another structure for the IMPI, which for example is not based on IMSI or MSISDN. In still another embodiment (not shown) PCCN (or PDF 33A or CRF 34A in PCCN as an alternative to a PCCN), may query the service data flow based credit control 36A in order to get a connection between the IMS identity and the MSISDN/IMSI received from the TPF.

Fig. 8A schematically illustrates another architecture in which the inventive concept is applicable. Such an architecture is for example described in TR 23.803. The charging and/or policy handling node here comprises a PCCN 30B with a PDF 33B and a CRF 34B communicating with an AF 20B over a merged Rx/Gq interface. The packet data support node including TPF functionality 11 here comprises a gateway 10B which in addition to the TPF functionality 11 also includes a PEP (Policy Enforcement Point)

functionality, 12. Communication between PCCN 30B and gateway GW 10B takes place over the merged interface Go/Gx. PCCN 30B communicates with OCS (Online Charging System) 36B with a Camel SCP 37B and Service Data Flow Based Credit Control means 38B over the Ry interface. GW 10B communicates with OSC 36B over the Gy interface. GW 10B also communicates with a charging gateway function $15B_1$ and a charging collection function $15B_2$ over the Gz interface.

Fig. 8B shows still another embodiment similar to that of Fig. 8A but with the difference that OSC and PCCN are merged into one node 30C, communicating with GW 10C over a merged interface comprising interfaces Gy/Go/Gx merged with one another. In other aspects Fig. 8B is similar to Fig. 8A and OCS/PCCN 30C communicate over a merged interface Gq/Rx with AF 20C and GW 10C communicates over Gz with charging gateway function $15C_1$ and charging collection function $15C_2$.

It should be clear that these figures are merely illustrated in order to show some additional examples on architectures in which the inventive concept can be applied.

Hence, according to the invention, through only a slight addition to existing FBC architectures or similar early IMS security can be provided for. Operators using FBC for non-IMS based services migrating towards IMS are given the opportunity to simply upgrade FBC instead of HSS and Radius server, which is very advantageous. The inventive concept involves no implications on for example a GGSN architecture e.g. IP address allocation or release as it is the case with the proposal given in TR 33.878 and there is also no need to introduce an idle timer in GGSN. According to the invention identities from IMS

can be connected to e.g. GPRS based identities by using Rx and Gx interfaces.

Fig. 9 is a flow diagram describing one implementation of the inventive concept. It is here supposed that an UE requests TPF for bearer service establishment, 100. In the request, the UE includes first UE identity related information, or if it is a secondary PDP-context request, the first UE identity related information is already stored in the node handling TPF. This is however known in the art.

TPF then sends a request for charging and/or policy rules to CRF or PDF, or a PCCN, depending on the applicable implementation, including said first UE identity related information, 101. CRF/PDF (or PCCN) stores the first UE identity related information in storing means, e.g. a table, 102. Subsequently CRF/PDF (or PCCN) identifies and installs, using said first UE identity related information and possibly other information as referred to above, the relevant charging and/or policy rules, 103. Then CRF/PDF (or PCCN) provides the charging and/or policy rules to TPF, 104. A Bearer Service Establishment Acceptance message is then sent from TPF to UE, 105. Once a bearer service has been established, it is supposed that UE sends a SIP message or a SIP request, e.g. a SIP invite, to an Application Function AF, 106. It may then be checked whether the private user identity is known from the SIP message, 107. If not, it may be derived somehow either in AF or in communication with some other node or function as discussed above, 107A. Then, as well as if the private user identity actually was known from the SIP message or SIP request, the second UE identity related information is sent to CRF/PDF or PCCN, 108. In CRF/PDF or PCCN it is thus then examined whether the first UE identity related information and the second UE identity related information

originate from one and the same UE, 109. If not, it is checked whether the charging and/or policy handling rules are to be deactivated, 109A, if yes, they are deactivated and/or the concerned traffic is discarded, 109B. If however the option is selected that the rules are not to be deactivated in step 109A, as well as if the first and the second UE identity related information respectively do originate from one and the same UE, the charging and/or policy rules are implemented, 110.

It should be clear that the invention is not limited to the specifically illustrated embodiments but that it can be varied in a number of ways within the scope of the appended claims.

CLAIMS

1. An arrangement in a communications system participating in user station service request and/or access procedures and comprising a number of packet data support nodes (GGSN;CGSN;TPF;10;10B;10C), a number of charging and/or policy handling nodes (CRF;TPF;PCCN;30;30A;30B;30C) and a number of application functions (AF;(P),(S),(I)CSCF;20;20B;20C) handling mobility management and call control of mobile user stations (UE;1) requesting and/or accessing services,

c h a r a c t e r i z e d i n

that the packet data support node(s) (10;10B;10C) comprise(s) means adapted to send first mobile user station (UE;1) identity related information over a first interface (Gx,Gy;Gx/Gy) to a charging and/or policy handling node (CRF;PDF;PCCN;30;30A;30B;30C), at reception of a request for bearer services from a mobile user station (UE;1),

that the application function(s) (AF;(P),(S),(I)CSCF;20;20B;20C) comprise(s) means for, at reception of a request for a service session (SIP) from a mobile user station (UE;1), sending second mobile user station identity related information to the charging and/or policy handling node (CRF;PDF;PCCN;30;30A;30B;30C), over a second interface (Rx,Rx/Gq),

and in that the policy and/or charging handling node (CRF;PDF;PCCN;30;30A;30B;30C), comprises verification means (32;32A) adapted to establish whether the request for a bearer service to the packet data support node (10;10B;10C) and the request for a service session to the application function (AF;P/S/I-CSCF;20;20B;20C) originate from one and the same mobile user station (UE;1).

2. An arrangement according to claim 1,

c h a r a c t e r i z e d i n
that the first mobile user station identity related information comprises one or more of MSISDN, IMSI and IP address of the mobile user station (UE;1).

3. An arrangement according to claim 1 or 2,
c h a r a c t e r i z e d i n
that the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU).

4. An arrangement according to claim 1 or 2,
c h a r a c t e r i z e d i n
that the second mobile user station identity related information comprises IMSI and/or MSISDN, e.g. derived from IMS private or public identity (IMPI,IMPU), or that the application function (20;20B;20C) is adapted to fetch said information externally, e.g. from a HSS.

5. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the IP addresses are received in, or derived from, the first mobile user station related information and the second mobile user station identity related information, and in that the verification means (32;32A) are adapted to compare the IP address obtained from the application function (20;20B;20C) with the IP address obtained from the packet data support node.

6. An arrangement according to claim 5,
c h a r a c t e r i z e d i n
that the verification means (32;32A) are adapted to, if required, establish and, use IMSI and/or MSISDN of said first and second

mobile user station identity related information respectively, to compare the associated IP addresses.

7. An arrangement according to claim 4,
c h a r a c t e r i z e d i n
that the charging and/or policy handling node (30;30A;30B;30C) is adapted to deduce IMSI and/or MSISDN from a received IMS private and/or public user identity (IMPI/IMPU).

8. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the charging and/or policy handling node (30;30A;30B;30C) is adapted to construe a private user identity using IMSI of a mobile user station, e.g. when no ISIM application is implemented.

9. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the charging and/or policy handling node (30;30A;30B;30C) is adapted to identify and install charging rules to be applied at reception of request therefor from a packet data support node (10;10B;15B_1,15B_2;10C.

10. An arrangement according to claim 9,
c h a r a c t e r i z e d i n
that if the first and second user identity related information do originate from one and the same mobile user station (UE;1), the charging and/or policy handling node (20;30A,36A;30B,36B;30C) is adapted to implement the provisioned charging rules.

11. An arrangement according to claim 9,
c h a r a c t e r i z e d i n
that if the first and second user identity related information do not originate from one and the same mobile user station, the

charging and/or policy handling node (20;30A,36A;30B,36B;30C) is adapted to reject the charging rules and/or deactivate implemented charging rules and discard concerned IP flow traffic, and in that it is adapted to inform the application function (20;20B;20C) that no PDP-context is available.

12. An arrangement according to claim 9,
c h a r a c t e r i z e d i n
that if the first and second user identity related information do not originate from one and the same mobile user station, the charging and/or policy handling node (30;30A;30B;30C) is adapted to select whether to activate or deactivate the charging rules in the packet data support node.

13. An arrangement according to any one of the preceding claims,
c h a r a c t e r i z e d i n
that the packet data support node (10;10B;10C) comprises a node handling Traffic Plane Functions (TPF).

14. A user according to claim 13,
c h a r a c t e r i z e d i n
that the packet data support node comprises a GGSN (10) implementing TPF.

15. An arrangement according to claim 13,
c h a r a c t e r i z e d i n
that the packet data support node comprises a CGSN implementing TPF.

16. An arrangement according to claim 13,
c h a r a c t e r i z e d i n
that it comprises a stand-alone node or a gateway node (10B;10C) handling TPF or TPF and policy enforcement (PEP).

17. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the charging and/or policy handling node (30;30A;30B;30C) comprises a CRF, a PDF or a PCCN.

18. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the first interface is Gx or Go/Gx merged with Gy if the charging and/or policy handling node (30A;30B) is merged with an OCS (36A;36B).

19. An arrangement according to any one of the preceding claims, c h a r a c t e r i z e d i n that the second interface comprises Rx or Rx merged with Gq.

20. A charging and/or policy handling node (30;30A;30B;30C) in a communications system supporting communication of packet data and arranged to communicate with an application function (20;20B;20C) and a packet data support node (10;10B;10C), c h a r a c t e r i z e d i n that it is adapted to receive first mobile user station identity related information from the packet data support node (10;10B;10C) at reception of a request for a bearer service from a mobile user station (UE;1) in the packet data support node (10;10B;10C), to receive second mobile user station identity related information from the application function at reception of a request for a service session therein, and in that it comprises verification means (32;32A) for establishing whether the request for a bearer service to the packet data support node (10;10B;10C) and the request for a service session to the application function (20;20B;20C) originate from the same mobile user station (UE;1).

21. A charging and/or policy handling node according to claim 20, characterized in that the first mobile user station identity related information comprises one or more of MSISDN, IMSI and IP address of the mobile user station.

22. A charging and/or policy handling node according to claim 20 or 21, characterized in that the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU) of the mobile user station or IMSI and/or that the handling node is adapted to derive IMSI and/or MSISDN from IMPI and/or IMPU and/or adapted to request said IMSI and/or MSISDN from the application function.

23. A charging and/or policy handling node according to any one of claims 20-22, characterized in that the verification means (32;32A) are adapted to compare the IP address corresponding to or included in the first mobile user station identity related information and the IP address corresponding to or included in the second mobile user station identity related information.

24. A charging and/or policy handling node according to claim 23, characterized in that the verification means (32;32A) are adapted to, if required establish and, use IMSI and/or MSISDN of said first and second mobile user station identity related information, to compare the associated IP addresses.

25. A charging and/or policy handling node according to claim 22,

c h a r a c t e r i z e d i n
that it is adapted to derive IMSI and/or MSISDN from a received IMS private and/or public user identity (IMPI/IMPU).

26. A charging and/or policy handling node according to any one of claims 20-25,
c h a r a c t e r i z e d i n
that it is adapted to construe a private user identity using IMSI of a mobile user station, e.g. when no IMSI application is implemented.

27. A charging and/or policy handling node according to any one of claims 20-26,
c h a r a c t e r i z e d i n
that it is adapted to identify and install charging rules to be applied at reception of a request therefor from a packet data support node (10;10B;10C).

28. A charging and/or policy handling node according to any one of claims 20-27,
c h a r a c t e r i z e d i n
that it is adapted to identify and install charging rules to be applied at reception of request therefor from a packet data support node (10;10B;10C), and if the first and second user identity related information do originate from one and the same mobile user station (1), it is adapted to implement the provisioned charging rules, and, if the first and second user identity related information do not originate from one and the same mobile user station,
it is adapted to reject the charging rules and/or deactivate implemented charging rules and discard concerned IP flow traffic, to inform the application function (20;20B;20C) that no PDP-context is available or, to select whether to deactivate the

charging rules in the packet data support node (10;10B;10C) or to keep them active.

29. A charging and/or policy handling node according to any one of claims 20-28,
characterized in
that it comprises a CRF, a PDF or a PCCN or a node with a similar functionality.

30. A method in controlling service access, in a communication system supporting communication of packet data and comprising a number of packet data nodes, a number of charging and/or policy handling nodes and a number of application functions handling mobility management and call control of mobile user stations requesting/accessing services, comprising the steps of:

- receiving a request for bearer services from a mobile user station in a packet data support node,
- sending, from the packet data support node, first mobile user station identity related information of the mobile user station to a charging and/or policy handling node,
- receiving, subsequently, before or substantially simultaneously, a request for a service session from the mobile user station in an application function,
- sending, from the application function, second mobile user station identity related information to the charging and/or policy handling node,
- establishing, in the charging and/or policy handling node, whether the request for a bearer service to the packet data support node and the request for a service session to the application function originate from the same mobile user station.

31. A method according to claim 30,

wherein the first mobile user station identity related information comprises one or more of the MSISDN, IMSI and IP address of the mobile user station, and wherein the second mobile user station identity related information comprises IMS private identity (IMPI) and/or IMS public identity (IMPU), or the second user identity related information comprises IMSI and/or MSISDN, e.g. derived from IMS private or public identity (IMPI,IMPU), or the application function is adapted to fetch said information from a HSS.

32. A method according to claim 30 or 31,
further comprising the steps of:

- establishing or finding IMSI and/or MSISDN of said first and second mobile user station identity related information,
- comparing at least part of said first and said second mobile user station identity related information with each other.

33. A method according to claim 30,31 or 32,
comprising the step of:

- comparing the IP addresses of said first and second mobile user station identity related information.

34. A method according to any one of claims 30-33,
comprising the step of:

- deriving IMSI and/or MSISDN from received IMS private and/or public user identities (IMPI/IMPU).

35. A method according to any one of claims 30-34,
comprising the step of:

- construing, in the charging and/or policy handling node, a private user identity using IMSI of the mobile user station, e.g. when no ISIM application is implemented.

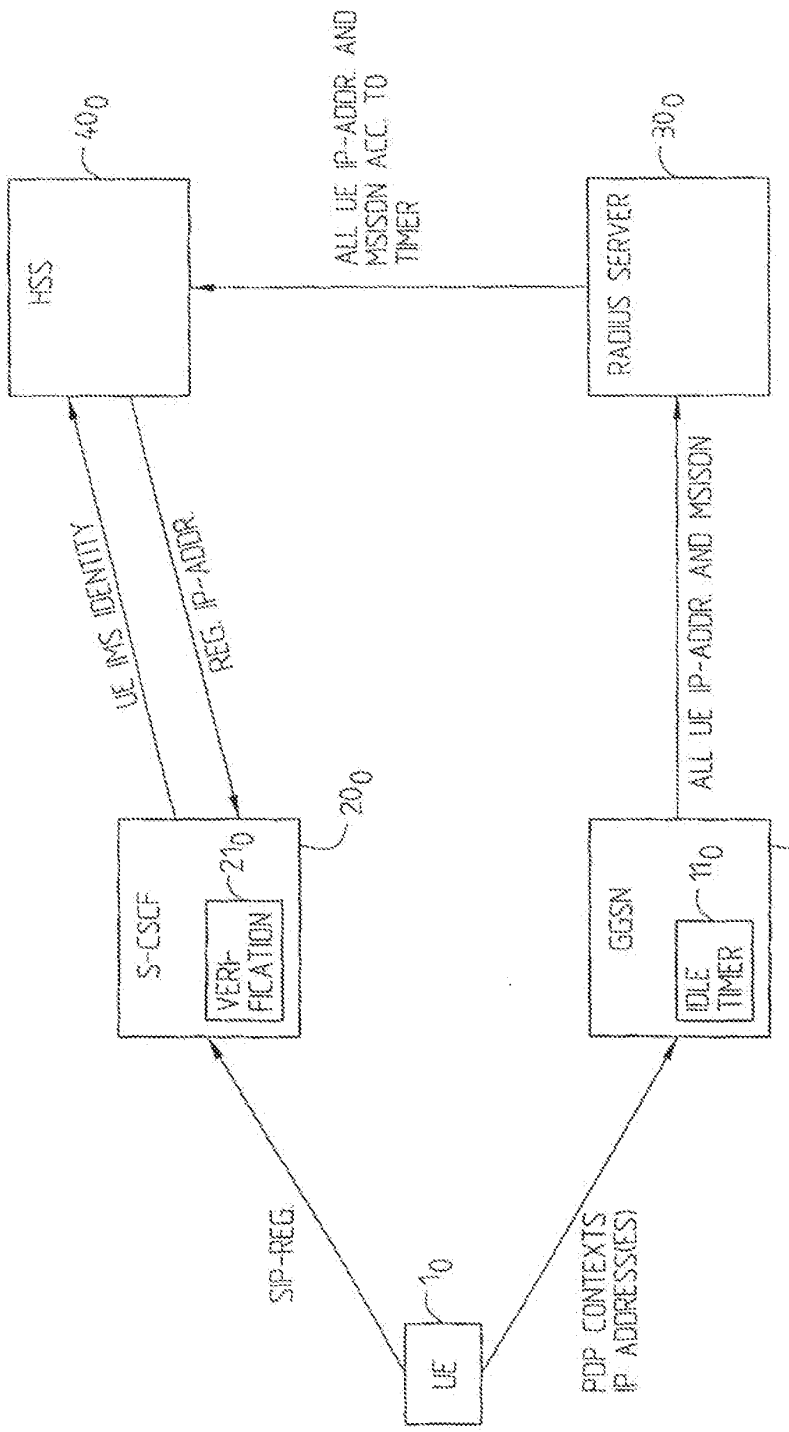
36. A method according to any one of claims 30-35, comprising the step of:

- identifying and installing applicable charging and/or policy rules at reception of a request from a packet data support node.

37. A method according to claim 36, further comprises the steps of:

- if the first and second mobile user station identity related information do originate from one and the same mobile user station,
- implementing the provisioned applicable charging rules and/or policy rules in the charging and/or policy handling node, otherwise,
- discarding concerned IP flow traffic, or
- selecting whether to activate or deactivate the charging rules.

38. A method according to any one of claims 30-37, wherein the packet data support node comprises a node handling Traffic Plane Functions, and is a stand-alone node, or a GGSN or a CGSN or a gateway node handling TPF and policy enforcement (PEP), and wherein the charging and/or policy handling node comprises a CRF, a PDF or a PCCN or a node with a similar functionality.



STATE OF THE ART

Fig. 1

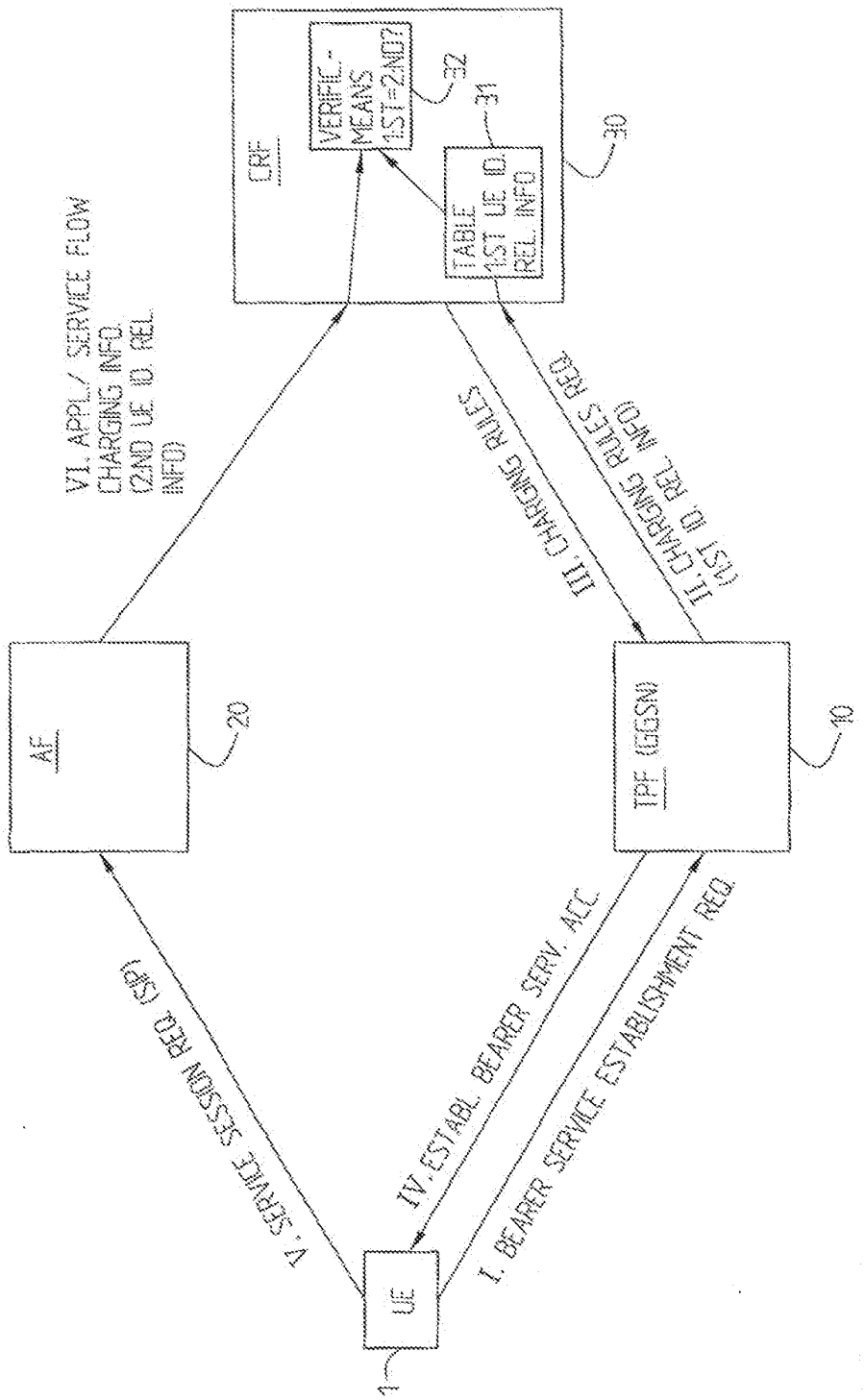

CRF
VERIFIC.-MEANS 1ST=2ND?
32
31
TABLE 1ST UE ID REL. INFO
30
V1. APPL./ SERVICE FLOW CHARGING INFO. (2ND UE ID, REL INFO)
III. CHARGING RULES
II. CHARGING RULES REQ (1ST ID REL INFO)
AF
20
TPF (GGSN)
10
V. SERVICE SESSION REQ (SIP)
IV. ESTABL. BEARER SERV. ACC.
I. BEARER SERVICE ESTABLISHMENT REQ.
UE
1

Fig. 2

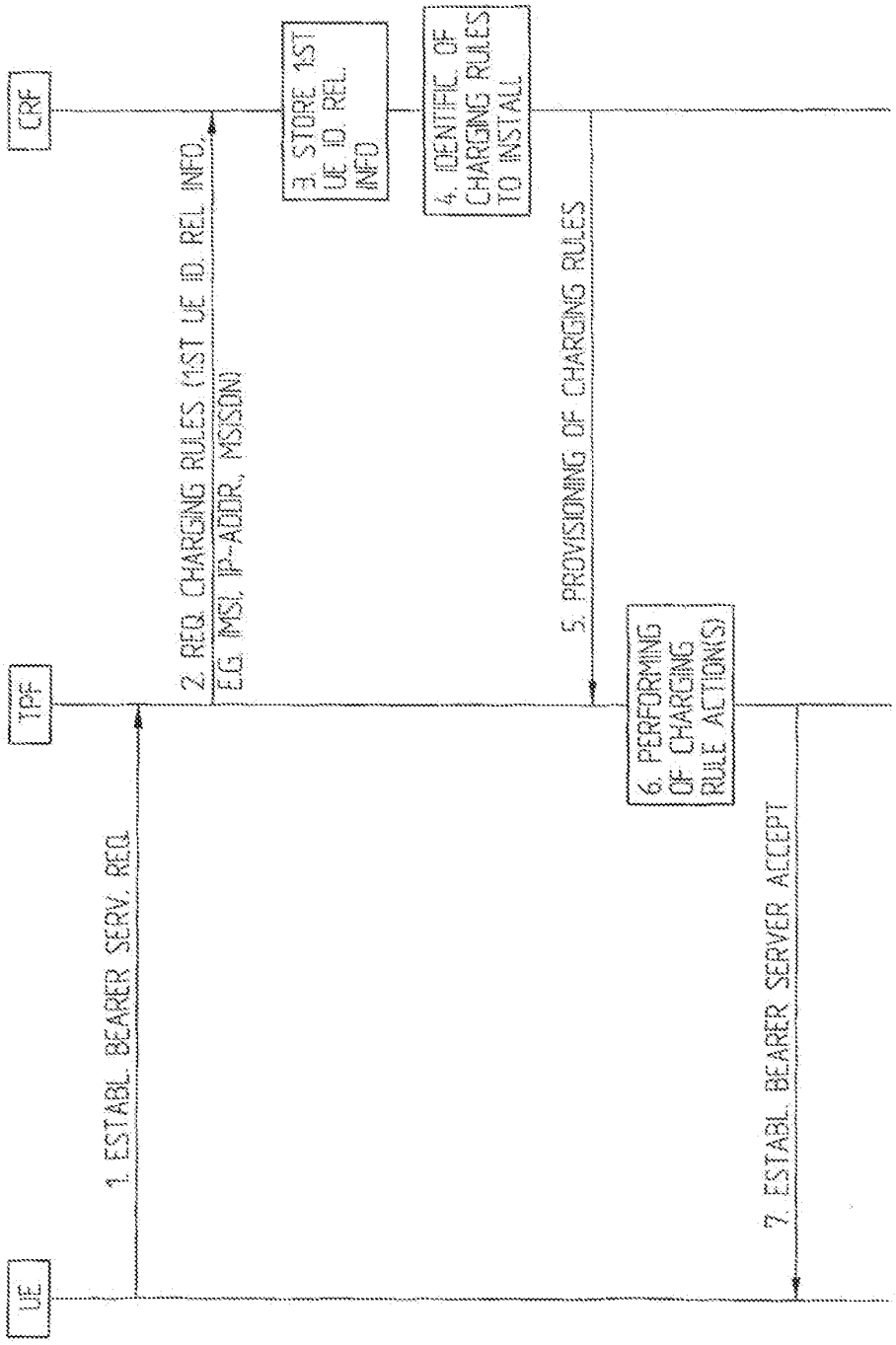

CRF
TPF
UE
1. ESTABL. BEARER SERV. REQ.
2. REQ. CHARGING RULES (1ST UE ID, REL INFO, E.G. IMSI, IP-ADDR, MSISDN)
3. STORE 1ST UE ID, REL INFO
4. IDENTIFC. OF CHARGING RULES TO INSTALL
5. PROVISIONING OF CHARGING RULES
6. PERFORMING OF CHARGING RULE ACTION(S)
7. ESTABL. BEARER SERVER ACCEPT

Fig. 3

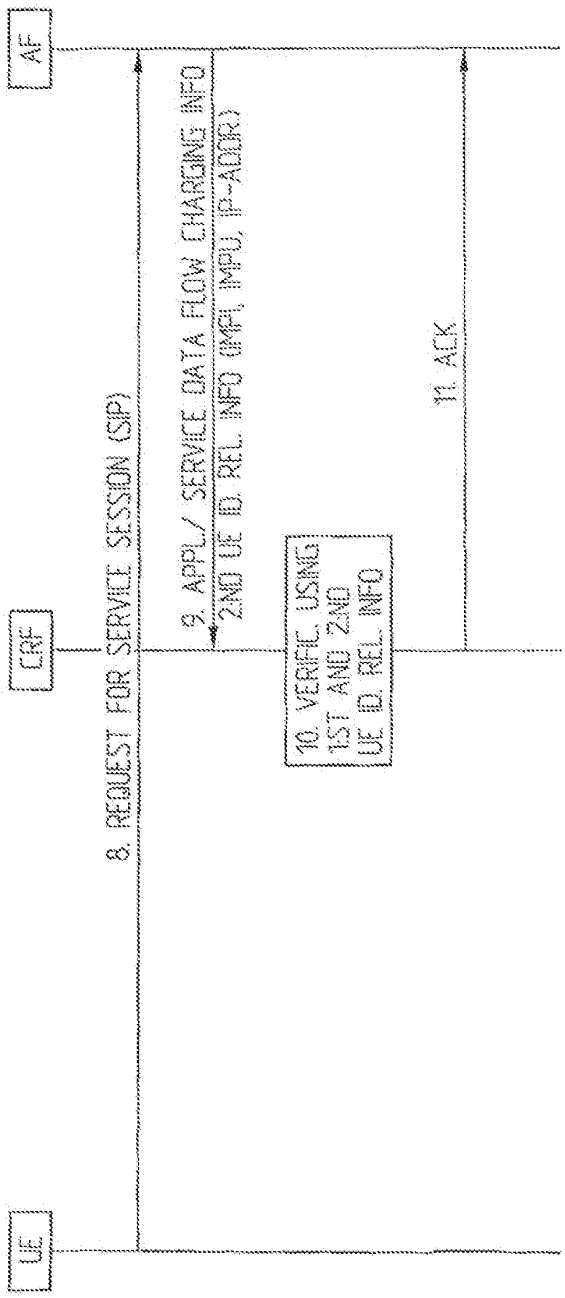

AF
CRF
UE
8. REQUEST FOR SERVICE SESSION (SIP)
9. APPL./ SERVICE DATA FLOW CHARGING INFO
2ND UE ID, REL. INFO (IMPI, IMPU, IP-ADDR.)
10. VERIFIC. USING
1ST AND 2ND
UE ID, REL. INFO
11. ACK

Fig. 4

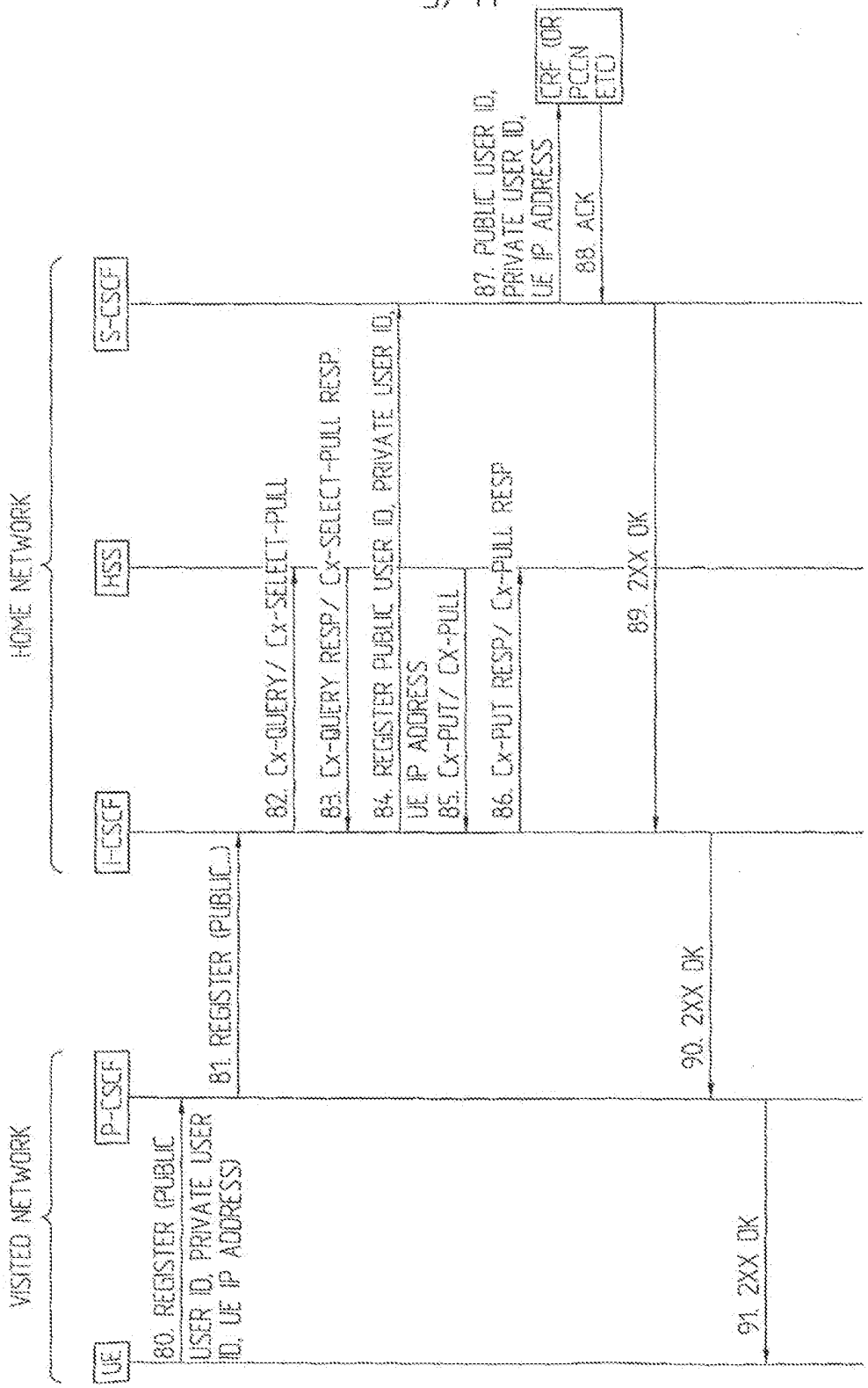

VISITED NETWORK
HOME NETWORK
UE
P-CSCF
I-CSCF
HSS
S-CSCF
80. REGISTER (PUBLIC USER ID, PRIVATE USER ID, UE IP ADDRESS)
81. REGISTER (PUBLIC...)
82. Cx-QUERY/ Cx-SELECT-PULL
83. Cx-QUERY RESP/ Cx-SELECT-PULL RESP.
84. REGISTER PUBLIC USER ID, PRIVATE USER ID, UE IP ADDRESS
85. Cx-PUT/ Cx-PULL
86. Cx-PUT RESP/ Cx-PULL RESP
87. PUBLIC USER ID, PRIVATE USER ID, UE IP ADDRESS
CRF (OR PCCN ETC)
88. ACK
89. 2XX OK
90. 2XX OK
91. 2XX OK

Fig. 5

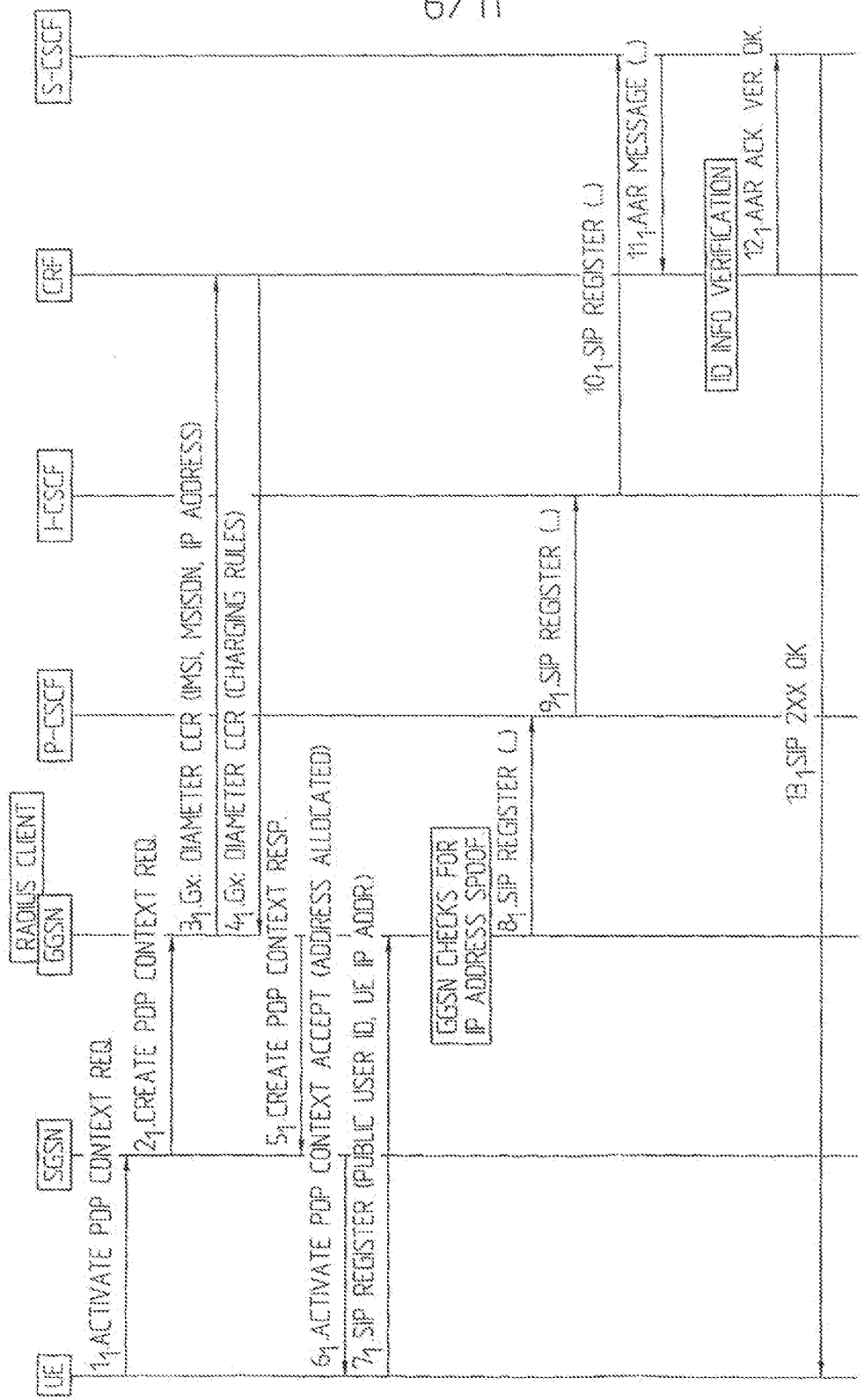

UE
SGSN
RADIUS CLIENT
GGSN
P-CSCF
I-CSCF
CRF
S-CSCF
1₁ ACTIVATE PDP CONTEXT REQ.
2₁ CREATE PDP CONTEXT REQ.
3₁ Gx: DIAMETER CCR (IMSI, MSISDN, IP ADDRESS)
4₁ Gx: DIAMETER CCR (CHARGING RULES)
5₁ CREATE PDP CONTEXT RESP.
6₁ ACTIVATE PDP CONTEXT ACCEPT (ADDRESS ALLOCATED)
7₁ SIP REGISTER (PUBLIC USER ID, UE IP ADDR)
GGSN CHECKS FOR IP ADDRESS SPOOF
8₁ SIP REGISTER (..)
9₁ SIP REGISTER (..)
10₁ SIP REGISTER (..)
11₁ AAR MESSAGE (..)
ID INFO VERIFICATION
12₁ AAR ACK. VER. OK.
13₁ SIP 2XX OK

Fig. 6A

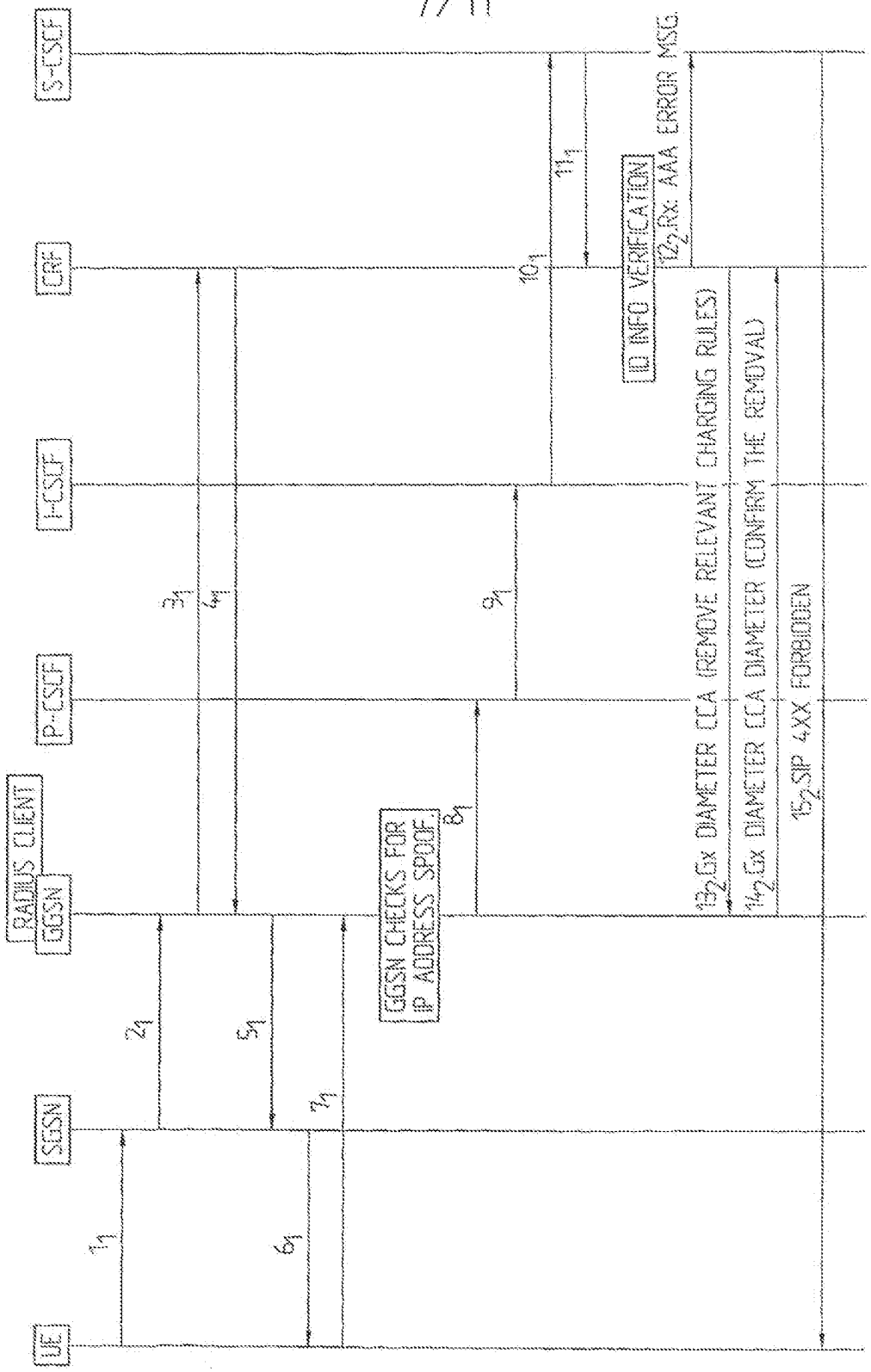

UE
SGSN
RADIUS CLIENT
GGSN
P-CSCF
I-CSCF
CRF
S-CSCF
1₁
2₁
3₁
4₁
5₁
6₁
7₁
8₁
9₁
10₁
11₁
12₂ Rx: AAA ERROR MSG
ID INFO VERIFICATION
13₂ Gx: DIAMETER CCA (REMOVE RELEVANT CHARGING RULES)
14₂ Gx: DIAMETER CCA (CONFIRM THE REMOVAL)
15₂ SIP 4XX FORBIDDEN
GGSN CHECKS FOR IP ADDRESS SPOOF

Fig. 6B

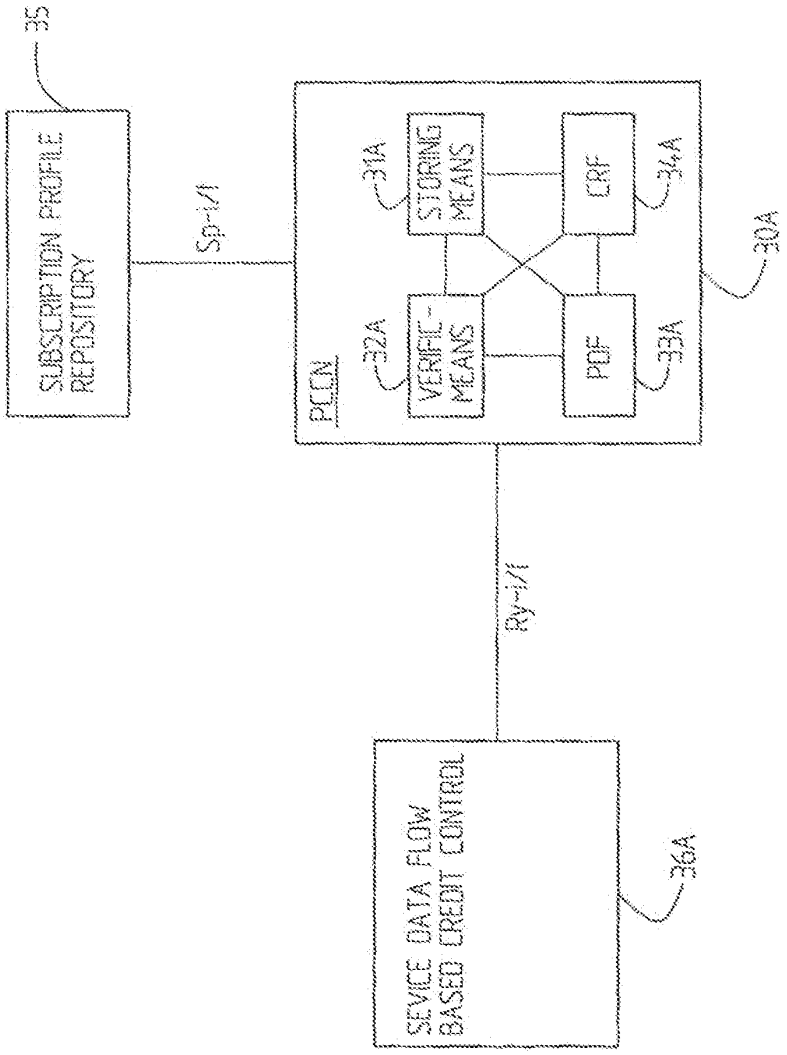

35
SUBSCRIPTION PROFILE REPOSITORY
Sp-i/f
PCEN
31A
STORING MEANS
CRF
34A
30A
32A
VERIFIC-MEANS
PDF
33A
Ry-i/f
SEVICE DATA FLOW BASED CREDIT CONTROL
36A

Fig. 7

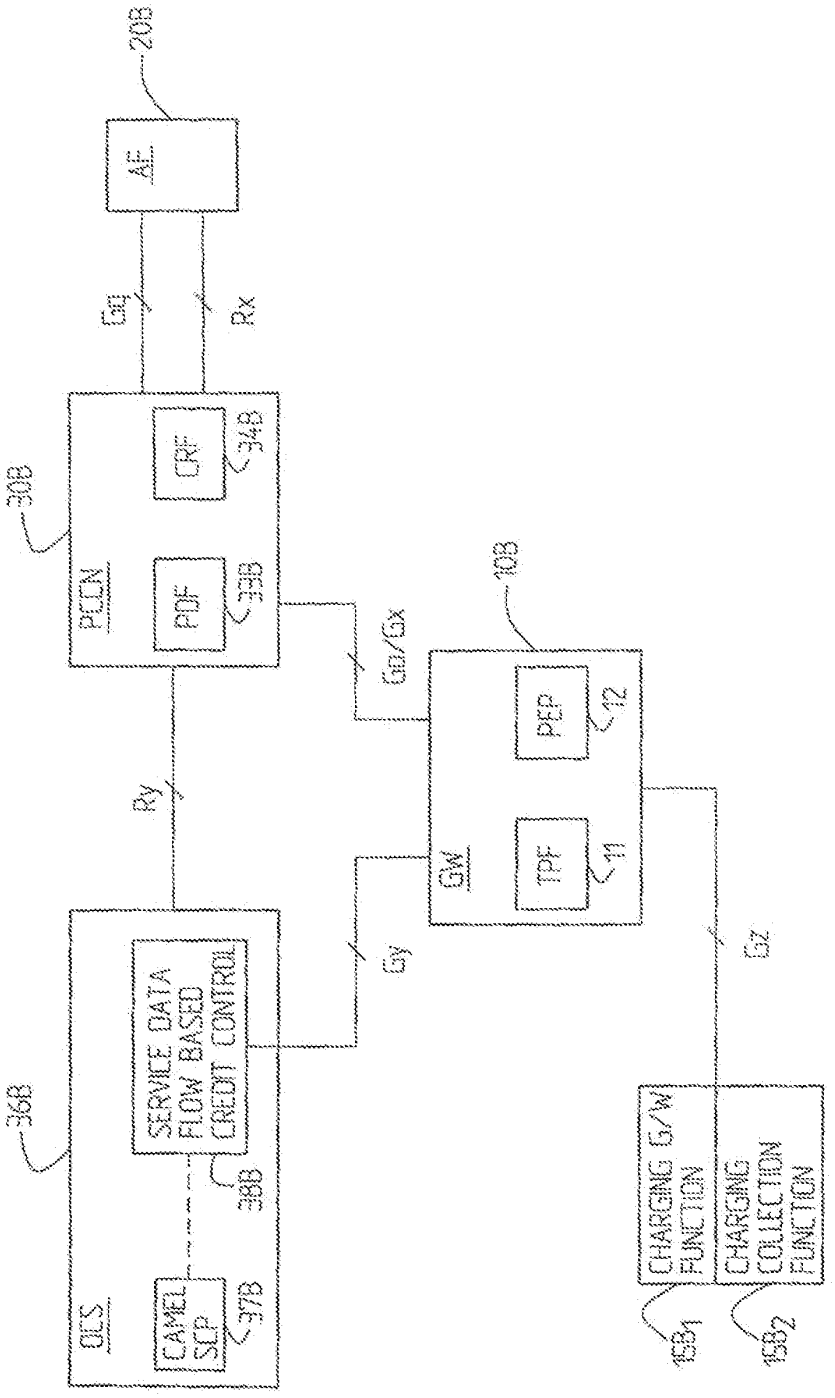

AF
20B
Gq
Rx
PCON
30B
CRF
34B
PDF
33B
Ry
Gx/Gx
10B
PEP
12
GW
TPF
11
Gy
Gz
OCS
36B
CAMEL SCP
37B
SERVICE DATA FLOW BASED CREDIT CONTROL
38B
CHARGING G/W FUNCTION
CHARGING COLLECTION FUNCTION
158₁
158₂

Fig. 8A

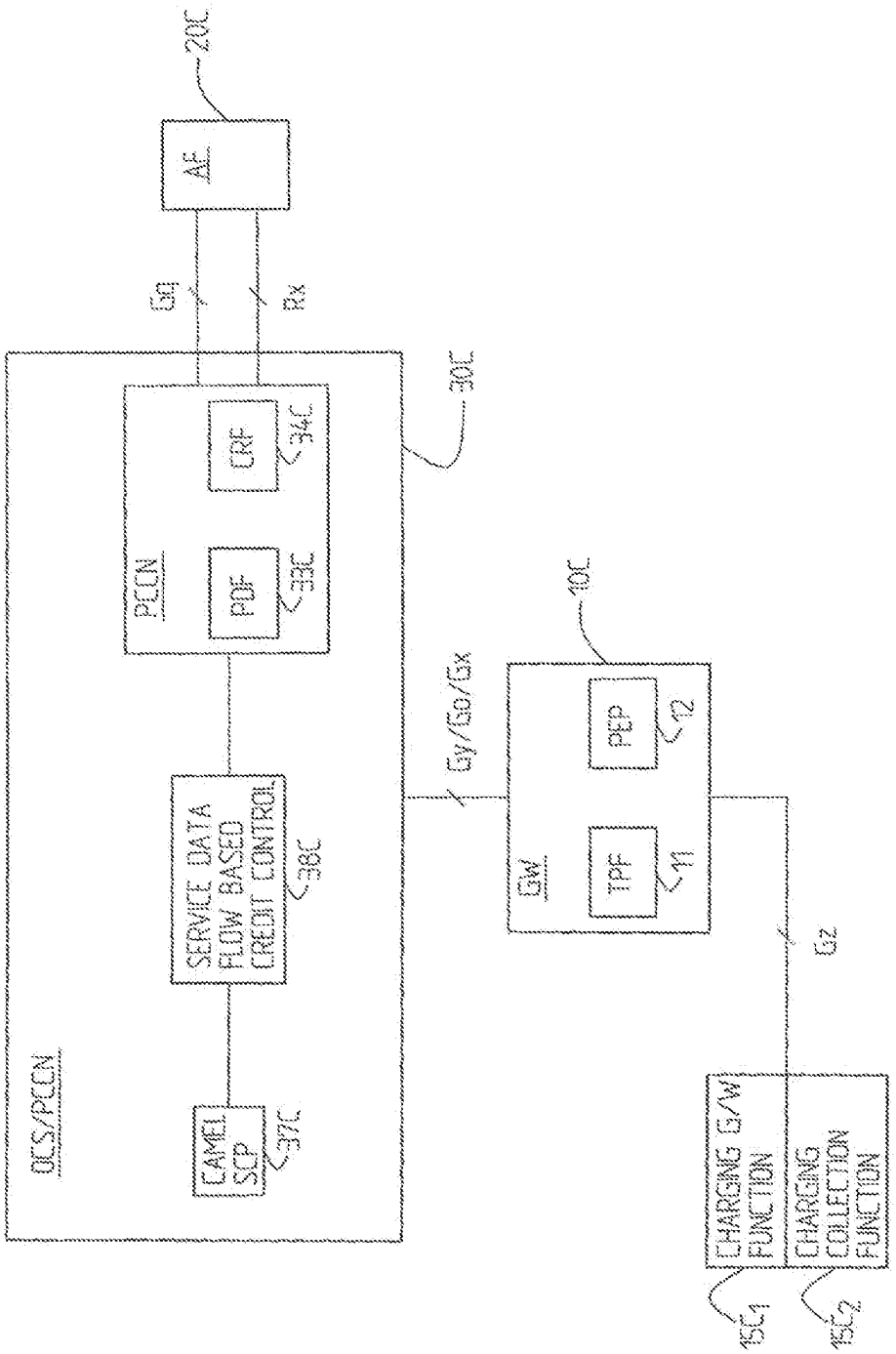

20C
AF
Gq
Rx
30C
PCCN
CRF
34C
PDF
33C
SERVICE DATA FLOW BASED CREDIT CONTROL
38C
CAMEL SCP
37C
OCS/PCCN
Gy/Gq/Gx
10C
GW
PEP
12
TPF
11
Gz
CHARGING G/W FUNCTION
CHARGING COLLECTION FUNCTION
15C1
15C2

Fig. 8B

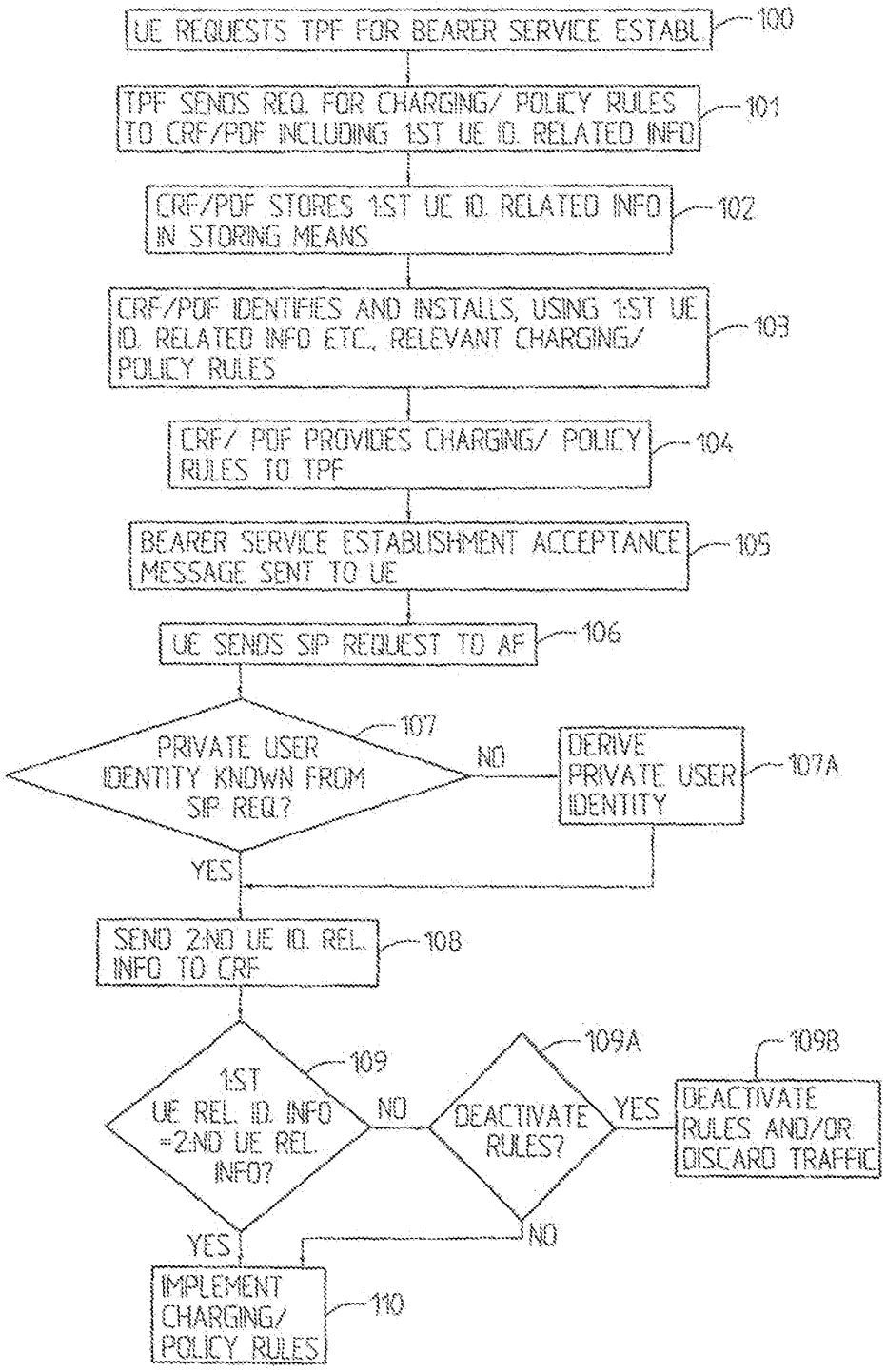

UE REQUESTS TPF FOR BEARER SERVICE ESTABL.
100
TPF SENDS REQ. FOR CHARGING/ POLICY RULES TO CRF/PDF INCLUDING 1ST UE ID. RELATED INFO
101
CRF/PDF STORES 1ST UE ID. RELATED INFO IN STORING MEANS
102
CRF/PDF IDENTIFIES AND INSTALLS, USING 1ST UE ID. RELATED INFO ETC., RELEVANT CHARGING/ POLICY RULES
103
CRF/ PDF PROVIDES CHARGING/ POLICY RULES TO TPF
104
BEARER SERVICE ESTABLISHMENT ACCEPTANCE MESSAGE SENT TO UE
105
UE SENDS SIP REQUEST TO AF
106
PRIVATE USER IDENTITY KNOWN FROM SIP REQ?
107
NO
DERIVE PRIVATE USER IDENTITY
107A
YES
SEND 2ND UE ID. REL. INFO TO CRF
108
1ST UE REL. ID. INFO =2ND UE REL. INFO?
109
NO
DEACTIVATE RULES?
109A
YES
DEACTIVATE RULES AND/OR DISCARD TRAFFIC
109B
NO
YES
IMPLEMENT CHARGING/ POLICY RULES
110

Fig. 9

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/002837

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04M H04Q

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01/91446 A (NOKIA CORPORATION; NOKIA INC) 29 November 2001 (2001-11-29) page 4, line 7 - page 5, line 2	1-38

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

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

'E' earlier document but published on or after the international filing date

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

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

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

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

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

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

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2005	06/07/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Veen, G

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/002837

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0191446 A	29-11-2001	US 2002127995 A1	12-09-2002
		CN 1444824 A	24-09-2003
		EP 1310085 A2	14-05-2003
		WO 0191446 A2	29-11-2001
		JP 2004507127 T	04-03-2004

Form PCT/ISA/210 (patent family annex) (January 2004)

Electronic Acknowledgement Receipt

EFS ID:	7930072
Application Number:	12380773
International Application Number:	
Confirmation Number:	5719
Title of Invention:	Verifiable service policy inplementation for intermediate networking devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	21912
Filer:	Michael J. Schallop/Veronica Pula
Filer Authorized By:	Michael J. Schallop
Attorney Docket Number:	RALEP018
Receipt Date:	01-JUL-2010
Filing Date:	02-MAR-2009
Time Stamp:	13:36:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	RALEP018_IDS_Before_1st_OA.pdf	56528 360846d02c00e598c3909f3171296226f661c34e	no	2
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Filed (SB/08)	RALEP018_IDS_SB08_1.pdf	124555 9cc6f6674c1f87436664a3391a757a65b3d4035a	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	RALE_Foreign_Ref_1A.pdf	6139391 ed22a6dbc67f09d4e7a5cb6045be867df9248ed8	no	49
Warnings:					
Information:					
4	Foreign Reference	RALE_Foreign_Ref_1B.pdf	2574136 928659e7726839520819 7f68febcdb55b01b915b	no	15
Warnings:					
Information:					
5	Foreign Reference	RALE_Foreign_Ref_1C.pdf	505198 81b92d38869e61daf2868357bed0ea81e29663a3	no	11
Warnings:					
Information:					
6	Foreign Reference	RALE_Foreign_Ref_1D.pdf	3048845 57a0856b7ec9abac7180d86595149dec996defdc	no	26
Warnings:					
Information:					
7	Foreign Reference	RALE_Foreign_Ref_1E.pdf	4616315 3e83c534eb55e82e478505c4d44bde2a72430854	no	34
Warnings:					
Information:					
8	Foreign Reference	RALE_Foreign_Ref_1F.pdf	5048671 cbad7159446ac414f1eeeed8214ef71e2adae8b4	no	38
Warnings:					
Information:					
9	Foreign Reference	RALE_Foreign_Ref_1G.pdf	5170774 c71740b2cd110174f5014e05d84acde040a43046	no	42
Warnings:					
Information:					
10	Foreign Reference	RALE_Foreign_Ref_1H.pdf	4124139 10eff1864a09668c5404e62fec900f25955b630d	no	36

Warnings:					
Information:					
11	Foreign Reference	RALE_Foreign_Ref_1I.pdf	3025460 60217d3f2867e38ce94f8f73ab1808b6938ba537	no	19
Warnings:					
Information:					
12	Foreign Reference	RALE_Foreign_Ref_1J.pdf	2632528 9240d5a44ab7e0daac9512d49a555fab8a37fb7d	no	13
Warnings:					
Information:					
13	Foreign Reference	RALE_Foreign_Ref_1K.pdf	7862034 663c74d022b4640fef56b6d06154d0afc06193e8	no	51
Warnings:					
Information:					
14	Foreign Reference	RALE_Foreign_Ref_1L.pdf	1929799 84c3744ddeee061cbb6a630d437dd3fc9d5f0a42	no	15
Warnings:					
Information:					
15	Foreign Reference	RALE_Foreign_Ref_1M.pdf	7699736 96ac86f4bbbc63af508f95f33927856e8c2f44c9	no	54
Warnings:					
Information:					
16	Foreign Reference	RALE_Foreign_Ref_1N.pdf	5831365 52c7919ee8f61002b63607e0b1afbb1c30411471	no	41
Warnings:					
Information:					
17	Foreign Reference	RALE_Foreign_Ref_1O.pdf	941474 84b1feb984dd76f2b40de9e9bf24bca6cbc317aa	no	18
Warnings:					
Information:					
18	Foreign Reference	RALE_Foreign_Ref_1P.pdf	4880569 cf0b517f0ea17a760054e4b34ec60d67a2caf375	no	37
Warnings:					
Information:					
19	Foreign Reference	RALE_Foreign_Ref_1Q.pdf	5439339 547fe6d96444a8d3f0953a82899a468dcaa3c29b	no	37

Warnings:					
Information:					
20	Foreign Reference	RALE_Foreign_Ref_1R.pdf	7122128 4ad5c3416c210e3f1efbd1c3e886d2ae2ad8e879	no	52
Warnings:					
Information:					
			Total Files Size (in bytes):	78772984	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Gregory G. Raleigh	Examiner:	Not Assigned
Application No.:	12/380,773	Art Unit:	2445
Filed:	March 2, 2009	Docket No.:	RALEP018
Title:	VERIFIABLE SERVICE POLICY IMPLEMENTATION FOR INTERMEDIATE NETWORKING DEVICES		

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§1.56 AND 1.97(b) BEFORE MAILING OF A FIRST OFFICE ACTION

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO SB/08, may be material to examination of the above-identified patent application. Applicants disclose these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application. Copies of the cited references are provided to the extent required by 37 CFR §1.98 and any applicable waivers.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is being filed (1) with the above-referenced application or (2) within three months of the filing date of the above-referenced application or (3) before the mailing date of a first Office Action on the merits or (4) before the mailing date of a first Office Action after filing of a Request for Continued Examination. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 50-0685 (Order No. RALEP018).

Respectfully submitted,
VAN PELT, YI & JAMES LLP

/Michael J. Schallop/

Michael J. Schallop
Registration No. 44,319
V (408) 207-4762
F (408) 973-2595

10050 N. Foothill Blvd, Ste 200
Cupertino, CA 95014

Substitute for form 1449/PTO				Complete if Known	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	12/380,773
				Filing Date	March 2, 2009
				First Named Inventor	Gregory G. Raleigh
				Art Unit	2445
				Examiner Name	Not Assigned
Sheet	1	of	2	Atty Docket No.	RALEP018

U.S. Patent Documents					
Examiner Initials	CiteNo.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS					
Examiner Initials	Cite No.	Foreign Patent Document Country Code–Number–Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	2A	WO 2006/077481	07-27-2006	True Context Corporation	
	2B	WO 2008/051379	05-02-2008	Verizon Services	
	2C	WO 2008/080139	07-03-2008	Integrated Mobile	
	2D	WO 2004/077797	09-10-2004	Boston Communications	
	2E	WO 2003/058880	04-17-2003	Telia AB	

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	2F	HARTMANN et al., Agent-Based Banking Transactions & Information Retrieval-What about Performance Issues? 1999	
	2G	VAN EIJK, et al., GigaMobile, Agent Technology for Designing Personalized Mobile Service Brokerage, July 1, 2002	
	2H	YU LI, Dedicated E-Reading Devices: The State of the Art and Challenges, Scroll, Vol. 1, No. 1, 2008	
	2I	DIKAIAKOS et al., A Distributed Middleware Infrastructure for Personalized Services, November 24, 2003	
	2J	RAO et al., Evolution of Mobile Location-Based Services, Communication of the ACM, December 2003	
	2K	CHANDRASEKHAR et al., Femtocell Networks: A Survey, June 28, 2008	
	2L	HOSSAIN et al., Gain-Based Selection of Ambient Media Services in Pervasive Environments, 2008	
	2M	Author Unknown, 3GPP TS 23.203, V8.4.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and Charging Control Architecture (Release 8), December 2008	
	2N	Author Unknown, 3GPP TS 23.401, V8.4.0, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packer Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 8), December 2008	
	2O	STEPHAN STEGLICH, I-Centric User Interaction, November 21, 2003	
	2P	HAN et al., Information Collection Services for Qos-Aware Mobile Applications, 2005	
	2Q	ALONISTIOTI et al., Intelligent Architectures Enabling Flexible Service Provision and Adaptability, 2002	
	2R	ROLF OPPLIGER, Internet Security: Firewalls and Bey, Communications of the ACM, May 1997, Vol. 40. No.5	

Substitute for form 1449/PTO				*Complete if Known*	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	12/380,773
				Filing Date	March 2, 2009
				First Named Inventor	Gregory G. Raleigh
				Art Unit	2445
				Examiner Name	Not Assigned
Sheet	2	of	2	Atty Docket No.	RALEP018

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[2] = Applicant is to place a check mark here if English language Translation is attached

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

(19) World Intellectual Property Organization
International Bureau

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

PCT

(10) International Publication Number
WO 2006/077481 A1

(51) International Patent Classification:
G06Q 10/00 (2006.01) *G06K 9/78* (2006.01)
H04L 12/16 (2006.01) *G06F 17/20* (2006.01)
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/IB2006/000076

(22) International Filing Date: 18 January 2006 (18.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/645,199 19 January 2005 (19.01.2005) US

(71) Applicant *(for all designated States except US)*: **TRUE-CONTEXT CORPORATION** [CA/CA]; 340 Maclaren Street, Suite 300, Ottawa, Ontario K2P 0M6 (CA).

(72) Inventors; and

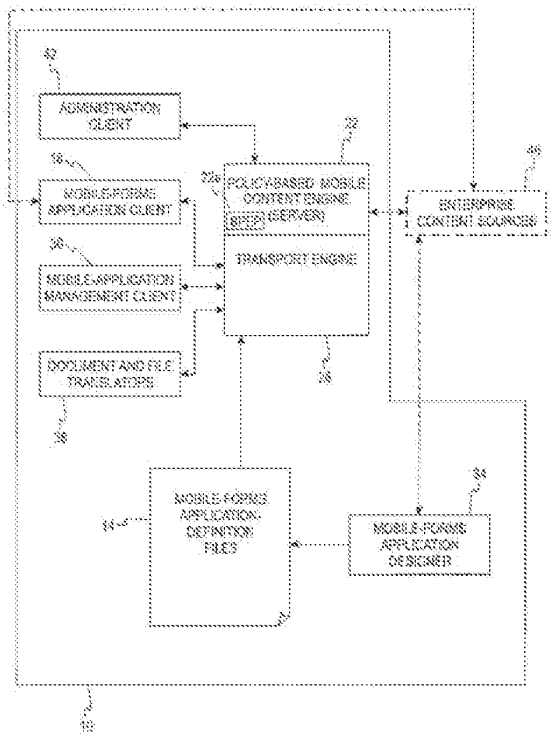
(75) Inventors/Applicants *(for US only)*: **CHANE, Marc** [CA/CA]; 111-29 Main Street, Ottawa, Ontario K1S 1B1 (CA). **MCGUIRE, Kevin** [CA/CA]; 41 Wimbledon Way, Ottawa, Ontario K2E 3J2 (CA). **PEYTON, Liam** [CA/CA]; 767 Rolling River Crescent, Ottawa, Ontario K1V 1M2 (CA).

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

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

[Continued on next page]

(54) Title: POLICY-DRIVEN MOBILE FORMS APPLICATIONS



(57) Abstract: A system for capturing data via an extensible markup language form is disclosed comprising a policy-based mobile content engine, a mobile-forms application client, and a transport engine. The policy-based mobile content engine is adapted to process a plurality of definitions from one or more mobile-forms application definition files. The policy-based mobile content engine translates the mobile-forms application definitions into policies and actions enforced by the policy-based mobile content engine. The mobile-forms application client has a plurality of rendering engines targeted for a mobile user device to render form controls and to process the forms-based application. The mobile-forms application client is operable on a mobile user device and is adapted to capture the data as an extensible-markup-language document. The transport engine is adapted to transport the mobile-forms application definition files and captured data through a transport layer between the policy-based mobile content engine and the mobile-forms application client.

WO 2006/077481 A1

Declaration under Rule 4.17:

- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

POLICY-DRIVEN MOBILE FORMS APPLICATIONS

FIELD OF THE INVENTION

[0001] The present invention relates generally to content management and, more particularly, to a system and method for defining, deploying, and managing mobile forms applications, in a multi-tenant (multi-domain) hosted environment, that can display and capture data on a wide variety of mobile devices in the context of a business workflow routed through a wide variety of intermittently connected networks both inside and outside of corporate firewalls.

BACKGROUND OF THE INVENTION

[0002] Today, most data in field force industries (e.g., field sales, field services, inspection and reporting, etc.) is distributed and captured on paper-based forms. The data entered on paper-based forms are typically returned to the business office to be manually entered electronically and integrated with a back office system. Furthermore, an enterprise business process might require the captured data to be reviewed by other members of the organization (e.g., authorization, up sell opportunity, billing, etc.) before, during, or after the field has interacted with the data. The process of distributing, updating, capturing, and returning form data and adapting it to a unique business process applies to a large number of mobile workers performing a variety of tasks such as, but not limited to, inspections (e.g., property, health, etc.), sales force reporting, and work order dispatches (e.g., HVAC, insurance claims, etc.).

[0003] Typically, in more complex forms-based business processes, work requests and form data are initially dispatched to field force workers using a voice channel (e.g., cell phone) or pre-printed paper forms (e.g., clipboard) that is then manually filled out or updated by the mobile worker (e.g., technician). A completed work request might also require one or many subsequent requests (e.g., required parts, required authorization, up-sell opportunities, etc.) that are typically done through a call over a cellular phone, or return trip to the office, or may cause the displacement of the mobile worker. Today, field inspectors may also capture data in the field using a series of paper forms and binders to complete their inspection tasks, resulting in a slow and inefficient process.

[0004] Businesses incur high wireless voice and vehicle fleet costs due to the above-described processes used in dispatching field workers, capturing or updating form data, and completing work orders or inspection forms in the field. Additionally, there are significant cost

and inefficiencies with slow, manual processes for the exchange of data using paper-based forms, from the cost of the paper based forms, to duplicate data entry, to errors made in data capture on paper, to waiting for the person with the data to update another person or system, etc.

[0005] Electronic forms and XForms (XML Forms) solutions (such as, Adobe LiveCycle, Microsoft Infopath, FormDocs, Alfova, Advantys, MDSI, X-Smiles, formsPlayer, and Novell XForms) are generally PC-centric and Local Area Network (LAN) oriented as opposed to being optimized for mobile devices and wireless use. Additionally, these solutions are on-line and browser-centric, as opposed to being optimized for on- and off-line use over intermittently connected wireless networks with varying degrees of cost and quality of service. These solutions typically do not provide mechanisms for hosting multi-tenants (multi-domain) forms applications using a common IT infrastructure (e.g., Managed Service Provider hosted environment), nor do they have support for sophisticated routing and tracking of forms and policies that define a mobile forms application.

[0006] Therefore, it would be desirable to have a system and method for defining, deploying, displaying, modifying, capturing, validating, and submitting/returning form data on mobile device using an intermittent network connection that addresses one or more of these issues.

SUMMARY OF THE INVENTION

[0007] According to one embodiment of the present invention, a system for capturing data via an extensible markup language form is disclosed. The system comprises a policy-based mobile content engine, a mobile-forms application client, and a transport engine. The policy-based mobile content engine is adapted to process a plurality of mobile-forms application definitions from one or more mobile-forms application definition files. The policy-based mobile content engine is adapted to translate the plurality of mobile-forms application definitions into policies and actions. The policy-based mobile content engine is adapted to enforce the policies and actions that have been translated. The mobile-forms application client has a plurality of rendering engines targeted for one or more mobile user device. The rendering engines utilize a forms application definition markup language to render form controls and to process the forms-based application. The mobile-forms application client is operable on the one or more mobile user device and is adapted to capture the data both online or offline as an extensible-markup-language document. The transport engine is adapted to transport the mobile-forms application

definition files and captured data through a transport layer between the policy-based mobile content engine and the mobile-forms application client.

[0008] According to another embodiment of the present invention, a method for defining and enforcing routing rules to define a business process workflow is disclosed. The method comprises the act of defining, via a mobile-forms application designer, a mobile-forms application-definition file that defines a mobile forms application by providing, (i) a mobile forms application definition markup language, (ii) an extensible-markup-language-based policy model that applies to one or more data instances that are to be captured, (iii) routing information specifying one or more targeted mobile user devices to deploy the mobile-forms application-definition file to, and (iv) a means of distribution of the forms-based application to targeted mobile users devices. The method further comprises the act of determining the routing rules for the business process workflow by reading, via a business process engine proxy, the mobile-forms application-definition file for the specified routing information and associated extensible-markup-language-based policy model. The method further comprises the act of enforcing, via a policy-based content management engine, the routing rules determined based on the defined and read mobile-forms application-definition file. The deployment, form interaction, routing, and management of the mobile forms application is automatically supported by reading, deploying, and enforcing the mobile-forms application-definition file.

[0009] According to yet another embodiment of the present invention, a method for recognizing data superimposed on a paper form is disclosed. The method comprises the act of scanning a paper based form to create a paper-based form template. The method further comprises the act of capturing the location of a form data instance element overlaid on the paper-based form template. The method further comprises the act of capturing the size of a form data instance element overlaid on the paper-based form template. The method further comprises the act of creating an input field based on the location and size of the form data instance element. The method further comprises the act of linking the paper-based form template to an application data model. The method further comprises the act of populating the paper-based form template with mobile-forms application data for a specific data instance in the input field.

[0010] The above summary of the present invention is not intended to represent each embodiment, or every aspect, of the present invention. Additional features and benefits of the present invention are apparent from the detailed description, figures, and claims set forth below.

Brief Description of the Drawings

[0011] FIG. 1 is an illustration of a content management system for mobile forms applications, according to one embodiment of the present invention.

[0012] FIG. 2 is an illustration of a mobile-forms based content management network, according to one embodiment of the present invention.

[0013] FIG. 3 illustrates a business process engine proxy integrated with a policy-based mobile content engine, according to one embodiment.

[0014] FIG. 4 is an illustration of a process for creating, transmitting, and receiving data via a mobile forms application, according to one embodiment of the present invention.

[0015] While the invention is susceptible to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and will be described in detail herein. It should be understood, however, that the invention is not intended to be limited to the particular forms disclosed. Rather, the invention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the invention as defined by the appended claims.

Detailed Description of the Illustrated Embodiments

[0016] According to one embodiment of the present invention, the content management system for mobile forms applications enables organizations to define and deploy mobile applications, forms, and business process workflow to mobile users across an enterprise or by using a Managed Service Provider (MSP) hosted environment. The content management system for mobile forms applications can be utilized without any programming language code being written or scripted since it is defined by policies, wizards, templates, and XML models. The content management system for mobile forms applications provides secure centralized control and support for hosting multiple security domains, while addressing all the complications of mobility (access outside the firewall, intermittently connected, wide variety of mobile devices and networks of varying capabilities, integration with existing business processes, IT infrastructure, etc.).

[0017] The content management system defines a mobile-forms-application definition model and associated tools for: (1) defining XML-based applications, forms, and business process workflow that are optimized for mobility; (2) for interacting with XML data in a mobile forms application instance with model-driven, mobile-device-optimized forms; (3) structuring and defining—with model-driven policies—the process for delivering, storing, managing, notifying and routing XML forms and associated form content (data, voice notes, photographs, sketches, GPS/location data, external data inputs—e.g., bar-code scanners, etc.) to and from users and systems for mobile forms applications; (4) managing and monitoring—with device-optimized interfaces—the status of XML mobile forms applications and all its instances, including support for on and off-line use; and (5) document-based translation of XML to and from a wide variety of forms for importing, exporting, transforming, and publishing the data and content associated with an instance of a XML mobile forms application.

[0018] The content management system for mobile forms applications leverages several XML standards and will be compatible with emerging XML standards in the area of business process management. However, the content management system for mobile forms applications provides innovation beyond what is defined in XML and XForms standards by addressing unique challenges presented by wireless and mobility (users, devices, networks, cost of service, quality of service, etc.). The content management system for mobile forms applications provides an automated, model-driven visual framework for the deployment and life-cycle management of mobile forms applications, and the processes associated with them (real-time and near-real time integration with structured and unstructured enterprise applications and content sources, configurable and dynamic notifications and alerts, routing of content, applications, and form data to and from mobile devices automatically or manually, etc.).

[0019] The policy-driven mobile forms applications have been designed and optimized for: (1) deployment and operation within an Enterprise or a hosted MSP environment for Enterprises (multi-tenant or multi-domain); (2) support for multiple types of OS-enabled PCs and mobile devices (beyond a PC/Laptop, including but not limited to Smartphones, PDAs, Handhelds, Tablet PCs, Handsets, Browser-based devices, Portable and Embedded terminals, etc.); (3) use behind the enterprise firewall (e.g. LAN, Wireless LAN, cradle) and while in the field (e.g., on/off-line, asynchronous mobile wireless network connections, Wide-Area Wireless connection, etc..); (4) use by non-technical users within every "role" (form design, business process owner,

end-user, administrators, etc.) and Small and Medium Sized Enterprises (SME's) as opposed to technical-users in enterprise IT departments and Large Enterprise Deployments; and (5) use without requiring extensive IT components needing to already be in place (e.g., middleware, enterprise content management, document and records management systems, databases, web servers, etc.).

[0020] Turning now to the drawings, FIG. 1 illustrates a content management system for mobile forms applications 10, according to one embodiment of the present invention. The content management system for mobile forms applications 10 includes eight main components: a plurality of mobile-forms application definition files 14; a mobile-forms application client 18; a policy-based mobile content engine (server) 22; a transport engine 26; a mobile-application management client 30; a mobile-forms application designer 34; a plurality of translators 38; and an administration client 42.

[0021] The mobile-forms application definition files 14, according to one embodiment, are specified in XML-based forms application definition markup language based on the W3C XForms specification to define a rich presentation of forms rendered in a Graphical User Interface (GUI) by the mobile forms application thick or thin-Client. Some enhancements have been made to extend the XForms schema to make it more efficient for mobile forms applications, as well as to support layout of form controls on mobile devices, and integrating routing of forms between users in a mobile forms application. An XML-based policy model is utilized by the mobile-forms application definition files 14 to define application and form states, workflow, validations, conditions, and actions to be processed for the life cycle of a new or updated form data instance. The policy model defines how the form data is managed (e.g., transformation and validation of data, publication of data to targeted resources, publication of data based on the type network connection, notifications and alerts to users based on form actions and events, etc.) and distributed, as well as to whom (people, systems, resources, etc.) it is distributed.

[0022] As discussed above, the mobile extensible forms markup language (mXForms) used in the mobile-forms application-definition files 14 is based on the XForms W3C recommendation (which can be found at http://www.w3.org/TR/2003/REC-xforms-20031014/). This mXForms markup language defines how to render rich GUIs online or offline for mobile devices, and display, update and captures data. mXForms and XForms distinctly define the presentation definition (look and feel), the format of the data captured, form controls, and the

behavior of the forms-based application (e.g., data validation, navigation, workflow, actions, etc.). It is a language that can fully leverage the limited display and functionality (including native and external peripherals—e.g., barcode scanner, GPS module, etc.) of some of the targeted mobile devices. Multiple views or mobile forms applications may be required to complete the data capture of a forms-based application, including support for contextual (e.g., dynamic) views or interaction with the form (e.g., Y happens only if the user has selected X in the form). Unique form controls are also needed to display, add, edit, and delete repeating line items on such limited devices. The markup language also affords for creation of unique form controls that future business processes may require. These multiple views and form controls can be used on- or off-line, via thin/thick clients on mobile devices that are OS-enabled.

[0023] The mobile-forms application client 18 includes a plurality of rendering engines targeted for each Operating System (OS) enabled mobile device or browser enabled device that can be used as a thick and thin client. The rendering engines use the XML-based forms application definition markup language to render a rich set of GUI form controls and to process the corresponding behavior of the forms-based application for the end-user. The rendering engines are adapted to create a fully configurable look and/or feel for the end-user. Furthermore, the mobile-forms application client 18 is capable of displaying (read-only or read/write), updating, and capturing the end-user's inputted data on- or off-line as one or more XML documents, as well as attachment files and managed lists that may be in a format other than XML.

[0024] The mobile-forms application client 18 is also able to display, update, capture and attach a wide variety of multi-media content to the form data. Alternatively or additionally, the rendering engines are adapted to encode this data to the XML form data instance as a base64 encoded element or reference the inputted text or binary file as a separate entity. The form data may include, for example, signatures, photos, voice notes, sketches, global positioning information, GoogleMaps, bar code scanning information, automobile monitoring information, etc.

[0025] For example, the mobile-forms application client 18 can call and control (interchange data) with an enabled device's Global Positioning System (GPS) coordinates to feed this information (as part of an XML form data instance or data blob) to the policy-based mobile content engine 22 (or to a forms solution). This data may then be used to assist in device

management—adding business value by allowing a user to, for example, locate a lost device or assist in locating and dispatching a desired field worker to a specific job. Additionally, GPS coordinates may be dispatched along with a work order to allow a field worker to utilize a mapping tool (e.g., GoogleMaps, MapPoint Location Server, etc.) to find the directions to the site for the work order. The mobile-forms application client 18 can pass this data to feed a mobile device application. For example, if the address of a dispatched work order is known, the mobile-forms application client 18 can pass this data to Microsoft PocketStreets and launch the application so the field worker can see the mapped address of their next work order. According to one embodiment, the bar code scanning information can be mapped to an input field within a form, or may be used to extract information from an external data source (e.g., a managed list, etc.). For example, the bar code information may represent a part number that can then be searched through a part list to extract the part's name, description, price, etc.

[0026] The content used by the mobile-forms application client 18 can either be embedded within the XML form data (base64 encoded) or be referenced and managed as attachment files in a very elegant way as content under the control of policies that control how the content is managed and distributed (e.g., don't force sending of large multimedia files associated with the form when the form is submitted wirelessly—unlike other database/sync or real-time forms solutions). The mobile-forms application client 18 can support a wide variety of technologies and input devices (e.g., Personal Digital Assistants (PDAs), smartphones, etc.) for data capture and form navigation. The input devices are linked to and interact with controls defined in the mobile extensible forms markup language to provide and enable data capture and form navigation.

[0027] By way of example, the mobile-forms application client 18, via the defined controls, are adapted to support a plurality of input devices, such as: keyboards (e.g., PC keyboard, keypad, Simple Input Panel (SIP), soft-keyboard, etc.); navigation, mouse, and I/O devices (e.g., optical mouse, RS-232 standard modules, touch-screens, scroll wheels, USB memory dongles, hard-drives, etc.); writing instruments and pointers (e.g., stylus, electronic pen/ink, handwriting to text conversion apps, etc.); audio (e.g., speech to text recognition, speech used the selection of an item from a list, speech used for form navigation using technology such as VRML, voice recorders, etc.); infrared reader; magnetic reader and cards (e.g., swipe card, proximity card, smart card, expandable media cards and storage devices such as, for example, SD, MMC,

compact flash, memory stick, etc.); Radio Frequency Identification (RFID); external or internal device peripheral (e.g., GPS, environmental meter, printers, etc.) including devices or data monitoring and reporting modules within an automobile (e.g., telematics); external or internal applications (e.g., VoIP softphone software, GPS software, etc.); scanners (e.g., optical character reader (OCR), bar code, biometric, etc.); incoming messages (e.g., via SMS, Smart Messages, OMA, SyncML, Email, SNMP, Active Sync, SMPP, SMTP, RSS/XML, etc.); and camera and digital imaging tools and devices.

[0028] The policy-based mobile content engine 22 includes a Business Process Engine Proxy (BPEP) 22a that processes mobile forms application definitions from the mobile-forms application definition files 14 and translates the application definitions into folder structures, files, and security roles as well as policies and actions that the policy-based mobile content engine 22 enforces. These policies and actions are utilized by the policy-based mobile content engine 22 to guide each instance of a mobile form through the business workflow process, including but not limited to, routing the form to different users and sending out notifications as the data fields of the mobile form are updated and actions are taken. The BPEP 22a uses the policy model (application data model, process states, user groups, folder structure, workflow, actions, conditions, etc.) defined in the mobile-forms application definition files 14. The policy model is extensible, flexible, visual, and may be wizard driven. As such, the policy model may be designed to be used and interacted with by non-technical users. Note that a mobile forms application is created by the BPEP 22a into a single security domain. The policy-based mobile content engine 22 explicitly represents the concept of multiple tenants (multiple domains) in its internal structures and partitions the content management, security roles, authorization, and policies associated with a mobile forms application by tenant (domain).

[0029] The transport engine 26 is an integrated client/server transport engine that is adapted to reliably transport (e.g., form data instance integrity and auditing of actions on the policy-driven mobile content engine 22 and mobile user device) the XML mobile application, forms data, and content through a configured transport layer (e.g., HTTP/HTTP(S), SyncML, ActiveSync, SOAP, FTP, SMTP, SMPP, RMI, IIOP, etc.) between the policy-based mobile content engine 22 and the mobile-forms application client 18. The transport engine 26 is optimized for mobility in regards to support for on- and off-line use, support for multiple OS-enabled mobile devices, support for various wireless and mobile networks with detection,

consideration and management for their various cost and quality of services, etc. Compression, byte differencing, and network policies (e.g., do not send large attachments when low bandwidth connection) are used to provide intelligent use of bandwidth. File caching, robust session management, partial file transmission support, and a robust synchronization protocol over HTTP are provided to address network unreliability.

[0030] The policy-based mobile content engine 22 addresses the challenges (limited and unique physical attributes, cost of service, quality of service, etc.) associated with wireless and mobile devices and networks through the use of network policies in conjunction with the transport engine 26. The transport engine 26 determines whether data compression should be used to minimize data transmitted over the transport layer as well as a number of other techniques (use right network at the right time, compression, byte-level differencing, check-point restart, caching and queuing of requests, automatic and manual client/server interactions, etc.)

[0031] The mobile-application management client 30 is made available on each Operating System (OS) enabled mobile device or browser enabled device that can be used as a thick and thin client.. The mobile-application management client 30 allows a manager or dispatcher to create, view, edit, assign, sort, search, or track the progress of form data for any given mobile forms application. The mobile-application management client 30 allows such functionality based on the information in the mobile-forms application-definition files 14. The mobile-forms application-definition files 14 map special "search fields" to information in a mobile form, including the current owner, the current state, as well as allowing custom defined fields. The mobile-application management client 30 leverages the folder structure and policies generated by the BPEP 22a, to display to a person managing mobile forms applications (e.g., dispatcher, office administrator, etc.) all the instances of a mobile form application, currently in progress. Additionally, the manager can see what state the mobile form is in, who it is assigned to, if the field worker has installed the right data on their device, etc. The mobile-application management client 30 incorporates the same rendering engine used by the mobile-form application client 18, so that a manager can select any form instance to view or edit it or create a new one. The manager can use this to change the status of a form or assign it to a different person.

[0032] The mobile-forms application designer 34 is adapted to create the mobile-forms application definitions contained within the mobile-forms application definition files 14. In particular, the mobile-forms application designer 34 allows a non-technical designer (having

minimal or no scripting, programming, or coding knowledge) to define an application in terms of: (i) the mobile forms application definition markup language; (ii) the XML-based policy model that applies to the captured data; (iii) the targeted OS-enabled mobile device (e.g., PCs, TabletPCs, Laptop, PDA, Smartphone, Handheld, Handset, Browser-enabled mobile device, etc.) or browser for the forms application definition; and (iv) the means of distribution of the forms-based application to targeted users (e.g., via push technology, SMTP, or available through a Uniform Resource Identifier (URI), etc.).

[0033] The mobile-forms application designer 34 is a simple Integrated Development Environment (IDE) for creating one or more mobile-forms application definition file 14. According to one embodiment of the current invention, the mobile-forms application designer 34 is a standalone PC-based application, but can also be an add-in to an existing application (e.g. Microsoft Visual Studio) or can be browser/web based. The data structure of the forms instance can be created by importing (e.g., via an enterprise content source) XML schema definitions or an instance of an XML file that is used as a demarcation point for back-end system integration. This includes flexible handling of version control and change propagation and data migration when refinements are made to the schema upon which a mobile forms application is based. The mobile-forms application designer 34 supports upgrades to a forms solution without disrupting the use of the forms solution by the field workers. Changes to the model shared between multiple participants are carefully migrated to the upgraded Data Instances (DIs) on the policy-based mobile content engine 22 transparently to the users of the forms solution. Version control on the DIs is important to understanding the data migration that needs to occur—possibly on the fly—at the time it is created and/or updated on the server by a field tech during the transition period until every field worker has the upgraded application/model on their user device.

[0034] The look and feel of the forms application is defined by the mobile-forms application designer 34. The form designer can create form-based applications using a rich set of form controls that can be dragged and dropped or defined on a single or multiple form view. The mobile-forms application designer 34 enables the use of drag and drop properties and other means and controls to define the form flow or navigation of the application. The form flow is how the user of the application can use a forms control (e.g., button, image, link, menu item, etc.) to modify forms. The form flow is mostly defined by an action added to a button. Conditional navigation can be controlled by the behavior typically defined by the "bind"

property of the control or the parent container of the control. The mobile-forms application designer 34 can associate actions to the form control to define the form flow.

[0035] The mobile-forms application designer 34 further defines a rich set of templates to speed the creation of or build forms (new or update forms) based application for specific OS-enabled targeted devices. This includes a translation service that helps with the automatic translation (and optimization) from a form optimized for one device into other devices (e.g., browser, laptop, etc.), as opposed to the user having to start from scratch for each device. The mobile-forms application designer 34 defines several wizards to simplify the steps to create, modify, copy, publish, test, etc. a forms based application and includes a test environment to process the authored mobile-forms application-definition files on the targeted device. Additionally, the mobile-forms application designer 34 provides workflow and form data validation, in one embodiment, through the search values and the predefined policies for a targeted participant for the workflow and the behavior as defined in XForms for validation.

[0036] The packaging of the forms application is provided by the mobile-forms application designer 34 as a simple installable application to any OS-enabled mobile devices (e.g., Windows NT/2000/XP/Tablet, Pocket PC, Win CE, etc.) or via a web-browser. The distribution of the forms application to system and non-system users via a BPEP 22a integrated with the policy-based mobile content engine 22 through push technology, SMTP, or a URI where the application can be downloaded, or rendered on the server and interacted with in a browser session.

[0037] The plurality of translators 38 are adapted to translate the mobile forms application instance data and content into a variety of formats (XML/HTML, PDF, SQL, CSV, Printers, Faxes, etc.) for further importing/exporting or for data manipulation, termination, or storage. A technique for form-based data superimposition recognition allows an author to define and automatically correlate the absolute positioning of form data, text, or image to be printed on a paper-based or electronic form template or layout.

[0038] A special design tool and document translator has been designed as part of this invention to facilitate the creation of a mobile forms application from existing paper-based forms. In typical paper-based processes, mobile workers collect data in paper forms that are faxed or printed. A mobile forms application also needs to use electronic data to print or fax a hard copy to the client on the same paper-based form. Existing print SDKs require absolute

positioning of objects (e.g., text, images) in order to position and size the captured form data sent it to a local printer to be printed on a template paper-based form.

[0039] The paper form data superimposition recognition is a special design tool and document translator that can scan existing paper-forms to create a document template and then link it to the application data model—through simple drag and drop or definition of data controls via the mobile-forms application designer 34. The mobile forms application data for a specific application instance can then be used to populate the template that is ready for printing or faxing. The paper form data superimposition recognition allows a designer to automatically build a forms application for a given forms solution using a scanned version of an existing paper-based form. The model and DI can automatically be generated using the paper-based form. In some embodiments, the paper form data superimposition recognition requires the designer to: (1) review the form and change the input fields to other types of form controls (e.g., text box changed to a date picker or a signature control); (2) define groups of repeated line items; etc.

[0040] The administration client 42 is adapted to allow an end-user administrator to setup the rights provided to a specific user or device, the groups the user or device belongs to, the content available to the user or device, the domains the user or device is able to access, etc. The administration client 42 is particularly useful in embodiments where a number of company's content and forms are located on the same policy-based mobile content engine 22. The end-user administrator can then use the administration client 42 to allow access to the company's content only to, for example, company employees. The administration client 42 transmits access rights to the policy-based mobile content engine 22 that then can limit the access to the content based on the user or device information of the user device trying to access the various content.

[0041] Typically, when a mobile form application is developed utilizing the mobile-forms application designer 34, the user information, groups, and access rights are generated as well. However, as the access rights change over time, the end-user administrator can utilize the administration client 42 to adjust the access rights, users, or groups accordingly. This allows the end-user's IT department to manage their content and resources in a secure, desirable, and efficient manner.

[0042] One or more enterprise content sources 46 are in communication with the policy-based mobile content engine 22. The one or more enterprise content sources 46 may also communicate with the mobile-forms application designer 34 or the mobile-forms application

client 18. The one or more enterprise content sources 46 are integrated directly with the policy-based mobile content engine 22, the mobile-forms application designer 34, and the mobile-forms application client 18 via a plurality of connectors.

[0043] The policy-based mobile content engine 22 can access the content and information stored on the one or more enterprise content sources 46 and transmit it to the various user devices based on the policies defined by the mobile-forms application-definition files 14. The mobile-forms application client 18 can utilize the one or more enterprise content sources 46 for pushing or receiving forms as XML files. Additionally, the mobile-forms application designer 34 can utilize the content contained with the one or more enterprise content sources 46 as a starting point for designing the mobile-forms application definition files 14.

[0044] Referring also to FIG. 2, a mobile-forms based content management network 60 is illustrated, according to one embodiment of the present invention. The content management network 60 allows the communication of the mobile-forms application client 18 with the policy-based mobile content engine 22 to transport the mobile-forms application-definition files 14 and all form data instances to and from a mobile device 64. The mobile-forms application client 18 is primarily comprised of a forms rendering engine that can present a user interface 68 as defined by in the mobile-forms application-definition files 14. The mobile-forms application-definition files 14 describe the user interface(s) 68 using the mobile extensible forms markup language that the forms rendering engine(s) interprets when displaying the user interface 68.

[0045] The mobile-forms application client 18 is available on a wide variety of OS-enabled mobile devices both as a native application 72 ("Thick Client") and as browser-enabled application 76 ("Thin Client"). It should be noted that even the browser-enabled applications are optimized to address the constraints of the devices they are operating on. The mobile-forms application client 18 communicates with the policy-based mobile content engine 22 via a client Application Programming Interface (API) to transport the mobile-forms application-definition files 14 and all form data instances 80 (associated XML data and content) to and from the mobile device.

[0046] As illustrated in FIG. 2, the policy-based mobile content engine 22, via the transport engine 26, delivers and receives the form data instances that are viewed and updated in the mobile-forms application client 18 (via the forms rendering engine) on a variety of devices 64, 72. Both "thick-client" 72 and "thin-client" 76 versions of the mobile-forms application client

18 leverage the transport engine 26 to communicate with the policy-based mobile content server 22 over intermittently connected networks 84 (sometimes online, sometimes offline). The communication consists mainly of delivering an instance of mobile form data, as well as mobile-forms application-definition files 14 to the mobile-forms application client 18 that determine how the mobile form data should be presented to the user. When the user updates the mobile form data instances 80, using the mobile-forms application client 18, they are communicated back to the policy-based mobile content engine 22 via the transport engine 26. Any changes to any instances are first persisted to a file prior to transporting them to the policy-base mobile content engine 22. This is done to ensure the user can safely keep working even if they are currently disconnected, to keep historical data on the device (if specified in the mobile forms application definition), and to provide a backup capability in case of device failure including but not limited to power failure such as no more battery power left.

[0047] Referring also to FIG. 3, the integration of the BPEP 22a with the policy-based mobile content engine 22 is further illustrated, according to one embodiment. A business process workflow is defined in one or more mobile-forms application-definition files 14 that are processed in the policy-based mobile content engine 22 via the BPEP 22a, according to one embodiment. The BPEP 22a is a component of the policy-based mobile content engine 22 that processes mobile forms applications and forms definitions. The mobile-forms application-definition files 14 used by the BPEP 22a can be defined by the non-technical form author using the mobile-forms application designer 34. When utilizing the mobile-forms application designer 34 the form author defines the states, workflow, and composition of the form data instance, the conditions that define the next state to process (e.g., if the technician requires new parts then go to state 'Y'), and the actions to be processed on a given state in the form's data instance life cycle.

[0048] For example, the following sample actions are supported by the mobile-forms application designer 34 and are capable of being interpreted by the BPEP 22a and enforced by the policy-based mobile content engine 22: content publication (e.g., add/move/copy/delete document or form data) to an existing/new network folder or other services (This action takes into account the user's access permissions to the document or form data on the targeted destination prior to publishing the content.); content auditing (auditing of user, device, and content information updated via the policy-based mobile content engine 22); content distribution

via email, fax, SMS, print and content push via the policy-based mobile content engine 22; content notification via email, fax, SMS, SNMP, SMPP, print, and/or other external web services; content transformation that may contain any other previously defined actions (It is possible to transform the data prior to distributing it via email (e.g., make it a viewable HTML document)); content validation (Some targeted devices might not support local validation against an XML schema. Therefore, the validation can be defined as an action and cause the document to be rerouted to the sender.); and network management (This action can require the sender to publish associated attachments to the data instance on a specific network type (e.g., EDGE/GPRS, UMTS, CDMA 1x, W-CDMA, WiFi, 802.11a/b/g, Bluetooth, LAN, cradle, etc.).).

[0049] According to one embodiment, the communication protocol of the content management system 10 utilizes HTTP(S) as the preferred protocol to transport all form data instance and attachments to the Policy-based Mobile Content Engine. The content management system 10 may utilize, as the preferred protocol to distribute and notify other internal or external resources (e.g., users, other machines, etc.), HTTP/HTTPS, SyncML, ActiveSync, SOAP, SMTP, FTP, SMS, SNMP, SMPP, RMI, IIOP, etc. Other communication protocols can be utilized without nullifying the key attributes of the above-described implementation. For example, web extensions such as SOAP and .NET can also be utilized, as well as proprietary communication protocols. The policy-based mobile content engine 22 may also act as an authorizing proxy for each of these protocols that allows the mobile-forms application client 18 to communicate in real time with one or more enterprise content sources 46 hosted behind the enterprise firewall. For example, a drop down list in a mobile form could be dynamically generated by a SOAP request to an enterprise content source 46. The policy-based mobile content engine 22 would apply appropriate policies both before and after routing the SOAP request from the mobile-forms application client 18 onto the enterprise content source 46.

[0050] The content management system 10 may utilize Secure Socket Layer (SSL) to encrypt all communication between the clients, other internal and external resources, and the policy-based mobile content engine 22. Other encryption techniques can be utilized without nullifying the key attributes of the invention. For example, a VPN tunnel could be used to secure the connection between the mobile-forms application client 18 and the policy-based mobile content engine 22. Similarly, an s-mime technique could also be adopted where the target

application is e-mail. Furthermore, the forms designer can specify that the data captured as an XML document on the mobile device may be encrypted using a public or secret-key cryptosystem (e.g., Kerberos, PKI, etc.) to properly secure the content on the mobile device if the device was stolen or lost, or if the policy-based mobile content engine 22 was compromised.

[0051] The content management system 10 enables existing authentication such as existing LDAP and RADIUS servers (local or remote, outside or behind the firewall with support for "single sign on" schemas) among others, to be used by the policy-based mobile content engine 22 to authenticate users of the mobile-forms application client 18, the mobile-application management client 30, and the administration client 42. The policy-based mobile content engine 22 can either automatically detect the required authentication or the policy-based mobile content engine 22 can be told by a system administrator to do so. Authorization providers are used to determine it the client is authorized based on their access permissions determined, but not limited to, the client's role and/or group access permission on the accessed resource (e.g. updating or creating a forms data instance).

[0052] The mobile-forms application designer 34 provides the end-user with custom-built form applications available on a thick or thin client. It also enables the forms designer to define all aspects of the mobile-forms application-definition files 14, target mobile devices, associate a test environment where the mobile-forms application-definition files 14 can be tested, associate business workflow, form navigation, behavior, data capture and define how the mobile forms applications can be procured and how they can be distributed, updated, or revoked from privileged users.

[0053] The content management system 10 provides superior end user, network, and client performance in several different ways. First, data compression may be used both in downloading newly dispatched and uploading updated form data instances. Furthermore, the policy-based mobile content engine 22 determines when file attachments associated with the mobile form application data instance should be delivered using both the type of network and attachment size. Additionally, the content management system 10 supports external model updates (e.g., customer list, price list, inventory list, etc.). These types of lists typically consist of a large amount of data that should only be updated at given times or when network availability permits. For more time critical updates to the list, byte level differencing and data compression can be used to update the end-users list with the changes rather than the updated list. This can reduce the network data

consumption by over 80% depending on the changes made to the list. Byte level differencing is done by transmitting only the changes between the old list and the new list (byte level differences) and by applying those changes as an update to the old list on the mobile device to create the new list on the mobile device. It can also be used to update an attachment to a form data instance.

[0054] The content management system 10 provides superior availability to mobile workers by enabling offline form filling when confined to areas with restricted network connectivity and by enabling online, near real time, updates of form data to the server. Further, the content management system 10 helps to ensure that forms application and associated resources (e.g., external lists) are pushed as mandatory items. The content management system 10 controls delivery of captured data instances and forms application on a device based on, but not limited to, network connectivity, time, etc. Near real time or scheduled updates to a mobile-forms application-definition file is enabled by, for example, using byte level differencing and data compression to reduce the size of the markup transported to the mobile device. The content management system 10 further enables automatic calculations, comparisons, enforced fields, data input limitations, mandatory fields, contextual form behavior, read-only and pre-filling of form data, thus assisting in speeding up data capture and business process completion.

[0055] As discussed above, the content management system for mobile forms applications 10 utilizes the mobile forms application markup language. The mobile forms application markup language can be utilized to define a number of enhanced form controls. For example, the mobile forms application markup language can define controls for: viewing the definition of a mobile-forms application-definition file 14 to better group controls and maximize display area of mobile devices with limited viewing area; providing new appearances for repeat line item controls; providing controls to view attachments; providing attributes to determine how an attachment is attached to the data instance (e.g., as a base 64 encoded, binary, or as a URI); providing support to display images; providing support to display links allowing form-view navigation or web page launch; providing a trigger with a background image; providing a toolbar with menu items used as a trigger or a submit XForms element; providing a header definition that allows the grouping of repeated controls used on different views; providing a footer definition that allows the grouping of repeated controls used on different views; and providing toolbar, header, and footer references used in a form-view definition to maximize limited resources on given devices (e.g.,

PPC). These controls can also be bound to dynamic real-time requests that are routed to enterprise content sources 46, via the policy-based mobile content engine 22.

[0056] Turning now to FIG. 4, a process for creating a mobile forms application, transmitting the mobile forms application, and receiving data via the mobile forms application is illustrated, according to one embodiment of the present invention. By utilizing the mobile-forms application designer 34 (FIG. 1), a non-technical user can define a mobile-forms application-definition file 14 (FIG. 1) at step 110. The mobile-forms application-definition file 14 defines the data model, form navigation, form validation, behavior, look and feel for the form application, and the various processing states that a form document will transition through. A mobile policy is also defined which specifies the rules and policies about routing, distribution, notification / alerts, devices, authorization, etc. All of these are created using a wizard-based, point-and-click interface, which requires no coding, scripting or programming on the part of the designer. There are also special tools for defining form based user interfaces that end-users can used to interact with application data, as well as special tools for defining format translations to import and export application data from XML into other formats (HTML, PDF, SQL, CSV, ASCII, etc.) including sending to a printer or fax. And there is a tool for importing, exporting, creating and editing XML schemas that define the structure of the data supported by the mobile-forms application-definition client 18. The mobile-forms application-definition file 14 is then stored to a hard disk.

[0057] The application data model, process states, folder structure, user groups, mobile policies, format translations, and user interfaces are all defined in XML-based mobile-forms application-definition files 14 that are generated onto the policy-based mobile content engine 22 at step 120. The policy-based mobile content engine 22 serves as a gateway between mobile forms applications and existing business processes, enterprise content sources, and applications.

[0058] The policy-based mobile content engine 22 automatically or manually can be used to create and set up folder structures at step 120a and to create user groups at step 120b. At step 120c, the mobile-forms application-definition file 14 is actually transferred to the policy-based mobile content engine 22. Information contained in the mobile-forms application-definition file 14 is used to define a folder structure in the policy-based mobile content engine 22, which will store the content associated with each application, and to define the user groups in the policy-

based mobile content engine 22, that will be allowed to access application data and content during the various processing states of an application instance.

[0059] The policy-based mobile content engine 22 generates a plurality of search and tracking fields at step 120d that allow a forms manager to look for and monitor the mobile forms applications that have been provided (and deployed) by the policy-based content management engine 22. At step 120e, the policy-based content management engine 22 generates client installation packages for installing the mobile form application onto the user devices. Routing and deployment policies are determined at step 120f by the policy-based content management engine 22 for the mobile form application based on the mobile-forms application-definition file 14. The policy-based content management engine 22 then generates a user's extensible-markup-language file at step 120g.

[0060] The mobile forms application created by the mobile-forms application designer 34, is deployed to the user devices at step 130 by the policy-based mobile content engine 22 (FIG. 1) and its associated transport engine 26 (FIG. 1). The deployment activates the mobile forms application such that the application and associated files, user lists, etc. will be pushed down to the user's mobile devices 64 (FIG. 2). Alternatively, the deployment may be accomplished by generating a media card (e.g., a SD card, mini-SD, etc.) along with user configuration files. The media card may then be utilized to automatically and intelligently install the mobile forms application and configuration files onto an OS-enabled user device. The deployment process manages both forms application upgrades as well as data migration that may be required for existing form instances persistent on the policy-based mobile content engine 22 and mobile devices.

[0061] The mobile-forms application client 18 (FIG. 1) is available on a wide variety of user devices (PC, Laptop, Tablet, PDA, Blackberry, Smartphone, Browser-based thin-client, etc.) that allows end-users to interact with application data and content. The mobile-application management client 30 (FIG. 1) is also available which allows managers to create, assign, and monitor application instances. Document translators 38 (FIG. 1) are used to view and print application data content, as well as transform it for use by other systems.

[0062] The policies of the mobile content engine are applied in response to any content management event (including, but not limited to reconcile requests from clients, new or updated files, files assigned to users, etc.). Policies are able to leverage whatever information is available

to the content management engine time in deciding what actions should occur (type of network, content or state of the files being transferred, users involved etc.). In particular, when a relevant state change is detected by the mobile application client 18 on a mobile device 64 (FIG. 2), the policy-based mobile content engine 22 is notified, and the policies for the particular mobile-forms application-definition file 14 are enforced at step 140. The state change may be, for example, the creation or modification of a form data instance 80 (FIG. 2) on the mobile device 64. The mobile-application management client 30 can be utilized at step 150 to create new form data instances and assign them to users (both actions will result in content management events that trigger the appropriate policies for the mobile forms application). Further, at step 150, the mobile-application management client 30 can be utilized to track the status of all data instances (e.g., what state they are in, who they are assigned to) using the search and tracking fields generated at step 120d.

[0063] Based on the policies relevant to the state change, the new or modified data instance can be transferred between the policy-based mobile content engine 22 and the user devices at step 160. This information can further be transferred between the policy-based mobile content engine 22 and the other user devices within the particular user group. The user or other users are then capable of interacting with the application data and content at step 170 once that information has been pushed to their user device by the policy-based mobile content engine 22.

[0064] This scenario is much more effective compared to other solutions that use data replication to synchronize databases on mobile devices with a central server database. First, such databases quickly become too big in practice given the limited capabilities of mobile devices. Second, a lot of unnecessary information is moved back and forth. Policy-driven mobile forms applications are designed to minimize the exchange of data wirelessly (use right network at the right time, compression, byte-level differencing, check-point restart, caching and queuing of requests, automatic and manual client/server interactions, etc.).

[0065] While the present invention has been described with reference to one or more particular embodiments, those skilled in the art will recognize that many changes may be made thereto without departing from the spirit and scope of the present invention. Each of these embodiments and obvious variations thereof is contemplated as falling within the scope of the claimed invention, which is set forth in the following claims.

WHAT IS CLAIMED IS:

1. A system for capturing data via an extensible markup language form, comprising:

a policy-based mobile content engine adapted to process a plurality of mobile-forms application definitions from one or more mobile-forms application definition files, the policy-based mobile content engine being adapted to translate the plurality of mobile-forms application definitions into policies and actions, the policy-based mobile content engine being adapted to enforce the policies and actions that have been translated;

a mobile-forms application client having a plurality of rendering engines targeted for one or more mobile user device, the rendering engines utilizing a forms application definition markup language to render form controls and to process the forms-based application, the mobile-forms application client being operable on the one or more mobile user device and being adapted to capture the data, as one or more form data instances, both online or offline as an extensible-markup-language document; and

a transport engine adapted to transport mobile-forms applications, definition files, and the captured data through a transport layer between the policy-based mobile content engine and the mobile-forms application client.

2. The system of claim 1, wherein the mobile-forms application client is further adapted to capture and attach a wide variety of multi-media content to the captured data.

3. The system of claim 1, wherein the plurality of rendering engines of the mobile-forms application client is adapted to encode the captured data as an extensible-markup-language form data instance.

4. The system of claim 1, wherein the plurality of rendering engines of the mobile-forms application client is adapted to reference the inputted data to an opaque object.

5. The system of claim 1, wherein the management and distribution of the captured data is controlled by one or more policy translated from the plurality of mobile-forms application definitions.

6. The system of claim 1, wherein the rendered form controls are linked to and interact with one or more input devices provided on the mobile user device, the one

or more input devices allowing for data capture and assisting with navigation of the forms-based application.

7. The system of claim 1, wherein the policy-based mobile content engine routes the one or more mobile-forms application-definition files to the mobile-forms application client via the transport engine.

8. The system of claim 1, wherein the policy-based mobile content engine sends notifications as one or more data field within the mobile-forms application definition files is updated.

9. The system of claim 1, wherein the policy-based mobile content engine supports multiple security domains in a hosted environment that enables mobile forms applications, folder structures, user groups, user authentication, policies, and form data instances to be partitioned and kept wholly separate by security domain.

10. The system of claim 1, wherein the transport engine utilizes data compression to transmit the mobile-forms application definition files and the captured data through the transport layer between the policy-based mobile content engine and the mobile-forms application client.

11. The system of claim 1, wherein the transport engine utilizes byte-level differencing when retransmitting or updating large files that are part of the mobile-forms application through the transport layer between the policy-based mobile content engine and the mobile-forms application client.

12. The system of claim 1, wherein the transport engine utilizes check-point restarting when transmit the mobile-forms application definition files and the captured data through the transport layer between the policy-based mobile content engine and the mobile-forms application client.

13. The system of claim 1, wherein the transport engine uses caching and queuing of requests for transmitting the mobile-forms application definition files and the captured data through the transport layer between the policy-based mobile content engine and the mobile-forms application client.

14. The system of claim 1, wherein the transport engine is able to support communication between the mobile-forms application client and the policy-based mobile content engine both inside and outside of a corporate firewall.

15. The system of claim 1, wherein the transport engine is able to maintain a secure and robust user session between the mobile-forms application client and the policy-based mobile content engine over an intermittently connected network, via file caching, partial file transmission support, and a robust synchronization protocol.

16. The system of claim 1, wherein the rendered form controls are linked to and interact with one or more enterprise content sources in real-time, a request to the one or more enterprise content sources being communicated either directly or via the policy-based mobile content engine.

17. A method for defining and enforcing routing rules to define a business process workflow, comprising:

defining, via a mobile-forms application designer, a mobile-forms application-definition file that defines a mobile forms application by providing,

(i) a mobile forms application definition markup language,

(ii) an extensible-markup-language-based policy model that applies to one or more data instances that are to be captured,

(iii) routing information specifying one or more targeted mobile user devices to deploy the mobile-forms application-definition file to, and

(iv) a means of distribution of the forms-based application to targeted mobile users devices;

determining the routing rules for the business process workflow by reading, via a business process engine proxy, the mobile-forms application-definition file for the specified routing information and associated extensible-markup-language-based policy model; and

enforcing, via a policy-based content management engine, the routing rules determined based on the defined and read mobile-forms application-definition file,

wherein the deployment, form interaction, routing, and management of the mobile forms application is automatically supported by reading, deploying, and enforcing the mobile-forms application-definition file.

18. The method of claim 17, wherein the extensible-markup-language-based policy model specifies a business process workflow including,

(i) definition of state attributes in terms of information contained in a mobile-forms application instance or information available at run time in the policy-based mobile content engine,

(ii) events triggered by a change to a state of the mobile forms application or requests to the policy-based mobile content engine,

(iii) conditional evaluation and responses to events, and

(iv) actions that can be processed either directly or via the policy-based mobile content engine, the actions including changing the state of the mobile-forms application client.

19. The method of claim 17 further comprising, allowing a manager to track the progress of a work request relative to the business process workflow by utilizing a mobile application manager client, the business process engine proxy, and the policy-based content management engine.

20. The method of claim 17 further comprising, sending dynamic alerts and notifications associated with a tracked business process workflow and other events.

21. The method of claim 17, wherein the mobile forms application designer is adapted to modify the mobile-forms application-definition file.

22. The method of claim 17, wherein the mobile forms application designer is adapted to modify the extensible-markup-language-based policy model.

23. The method of claim 17, wherein the mobile forms application designer is adapted to test and package a mobile-forms application-definition file and the mobile-forms application-definition file's dependencies.

24. The method of claim 17, wherein the routing information specifying one or more targeted mobile user devices specifies one or more groups of users.

25. The method of claim 17, wherein the mobile-forms application-definition file is a self-extractable packaged file.

26. The method of claim 17 further comprising, updating the mobile-forms application-definition file and providing the updated mobile-forms application-definition file to the mobile user device, via the policy-based content management engine and an associated transport engine.

27. The method of claim 26, wherein the updated mobile-forms application-definition file is provided to the mobile user device utilizing wireless network connectivity.

28. The method of claim 26, wherein a form instance data definition modification can trigger data migration of existing form data instances persistent on the policy-based content management engine and the mobile user devices to validate against a new forms instance data definition via the business process workflow.

29. The method of claim 17 further comprising, mapping, via one or more translator, the mobile forms application from the extensible forms language into a format preferred by a user.

30. The method of claim 17 further comprising, mapping, via one or more translator, the mobile forms application from the extensible forms language into a format appropriate for the mobile user device the mobile forms application is deployed on.

31. A method for recognizing data superimposed on a paper form comprising:

scanning a paper based form to create a paper-based form template;

capturing the location of a form data instance element overlaid on the paper-based form template;

capturing the size of a form data instance element overlaid on the paper-based form template;

creating an input field based on the location and size of the form data instance element;

linking the paper-based form template to an application data model; and

populating the paper-based form template with mobile-forms application data for a specific data instance in the input field.

32. The method of claim 31, wherein the input field can be changed from a generic input field to a form controlled field.

33. The method of claim 32, wherein the form controlled field is a date picker.

34. The method of claim 32, wherein the form controlled field is a signature control.

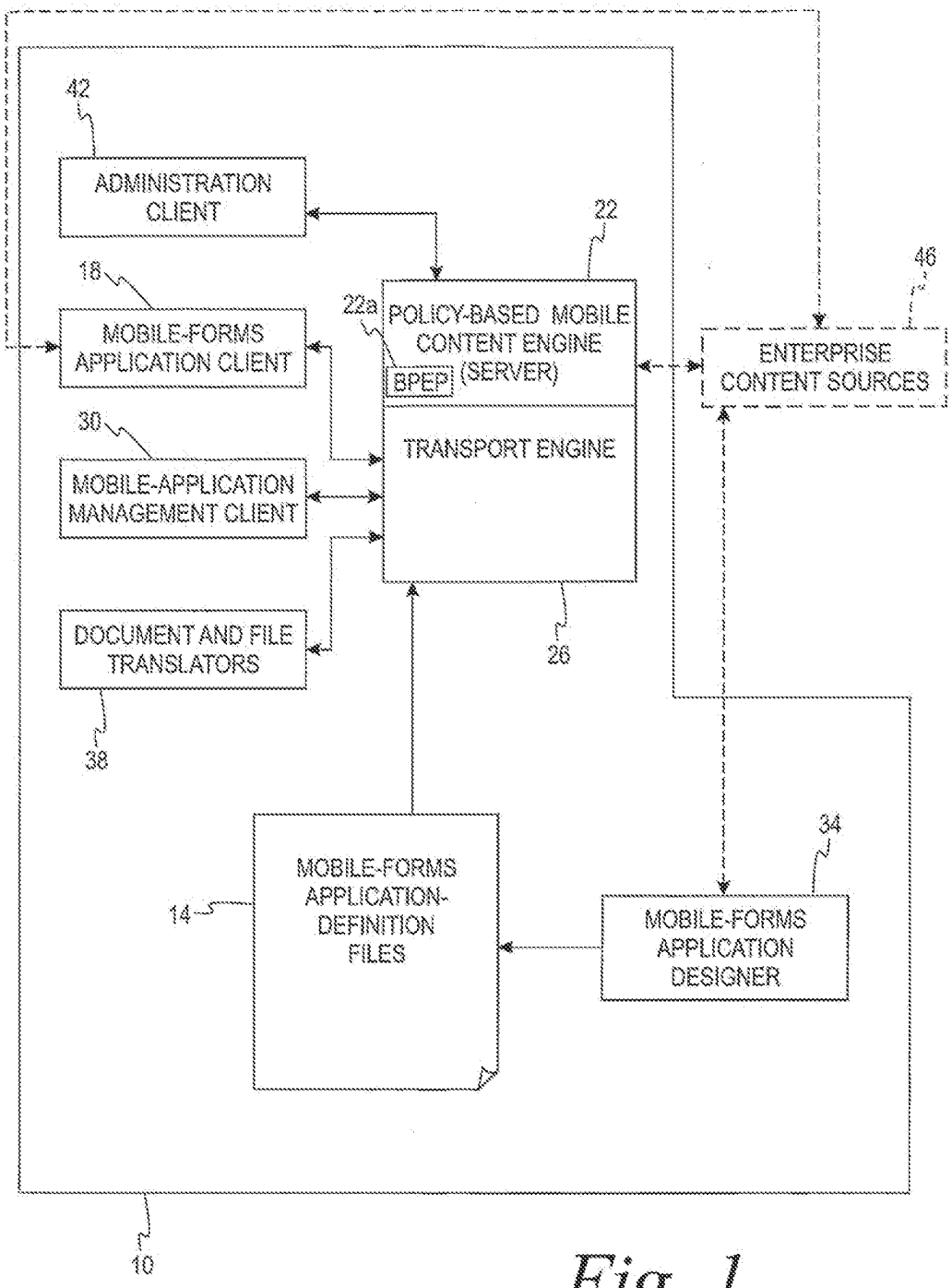

42
ADMINISTRATION CLIENT
22
46
18
22a
POLICY-BASED MOBILE CONTENT ENGINE
BPEP
(SERVER)
MOBILE-FORMS APPLICATION CLIENT
ENTERPRISE CONTENT SOURCES
30
TRANSPORT ENGINE
MOBILE-APPLICATION MANAGEMENT CLIENT
DOCUMENT AND FILE TRANSLATORS
26
38
34
14
MOBILE-FORMS APPLICATION-DEFINITION FILES
MOBILE-FORMS APPLICATION DESIGNER
10

Fig. 1

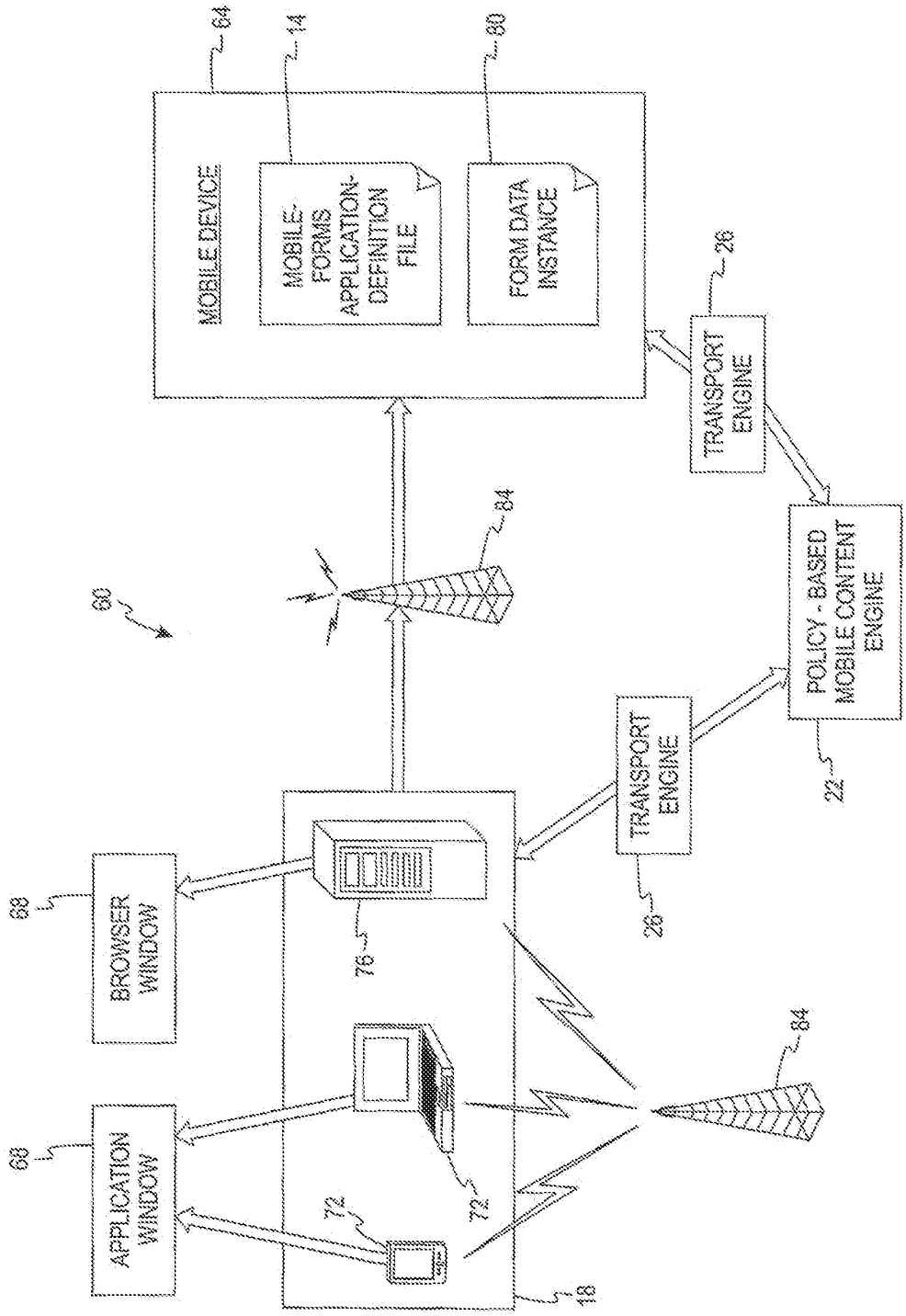

64
14
80
MOBILE DEVICE
MOBILE-FORMS APPLICATION-DEFINITION FILE
FORM DATA INSTANCE
26
TRANSPORT ENGINE
84
60
POLICY - BASED MOBILE CONTENT ENGINE
22
TRANSPORT ENGINE
28
68
BROWSER WINDOW
76
68
APPLICATION WINDOW
72
72
84
18

Fig. 2

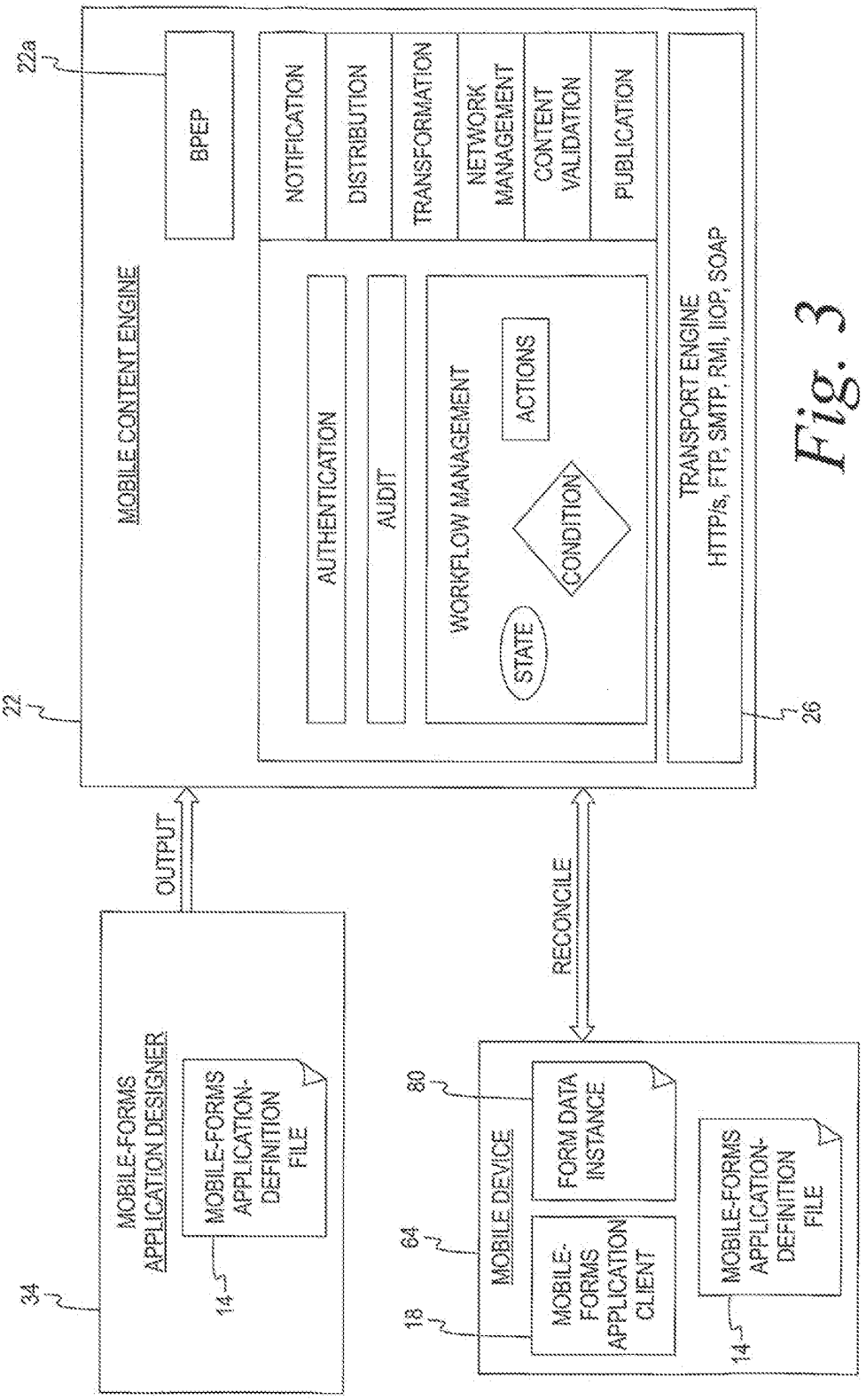

22a
MOBILE CONTENT ENGINE
BPEP
NOTIFICATION
DISTRIBUTION
TRANSFORMATION
NETWORK MANAGEMENT
CONTENT VALIDATION
PUBLICATION
AUTHENTICATION
AUDIT
WORKFLOW MANAGEMENT
ACTIONS
STATE
CONDITION
TRANSPORT ENGINE
HTTP/s, FTP, SMTP, RMI, IIOP, SOAP
22
26
OUTPUT
RECONCILE
34
MOBILE-FORMS APPLICATION DESIGNER
MOBILE-FORMS APPLICATION-DEFINITION FILE
14
18
64
80
MOBILE DEVICE
MOBILE-FORMS APPLICATION CLIENT
FORM DATA INSTANCE
MOBILE-FORMS APPLICATION-DEFINITION FILE
14

Fig. 3

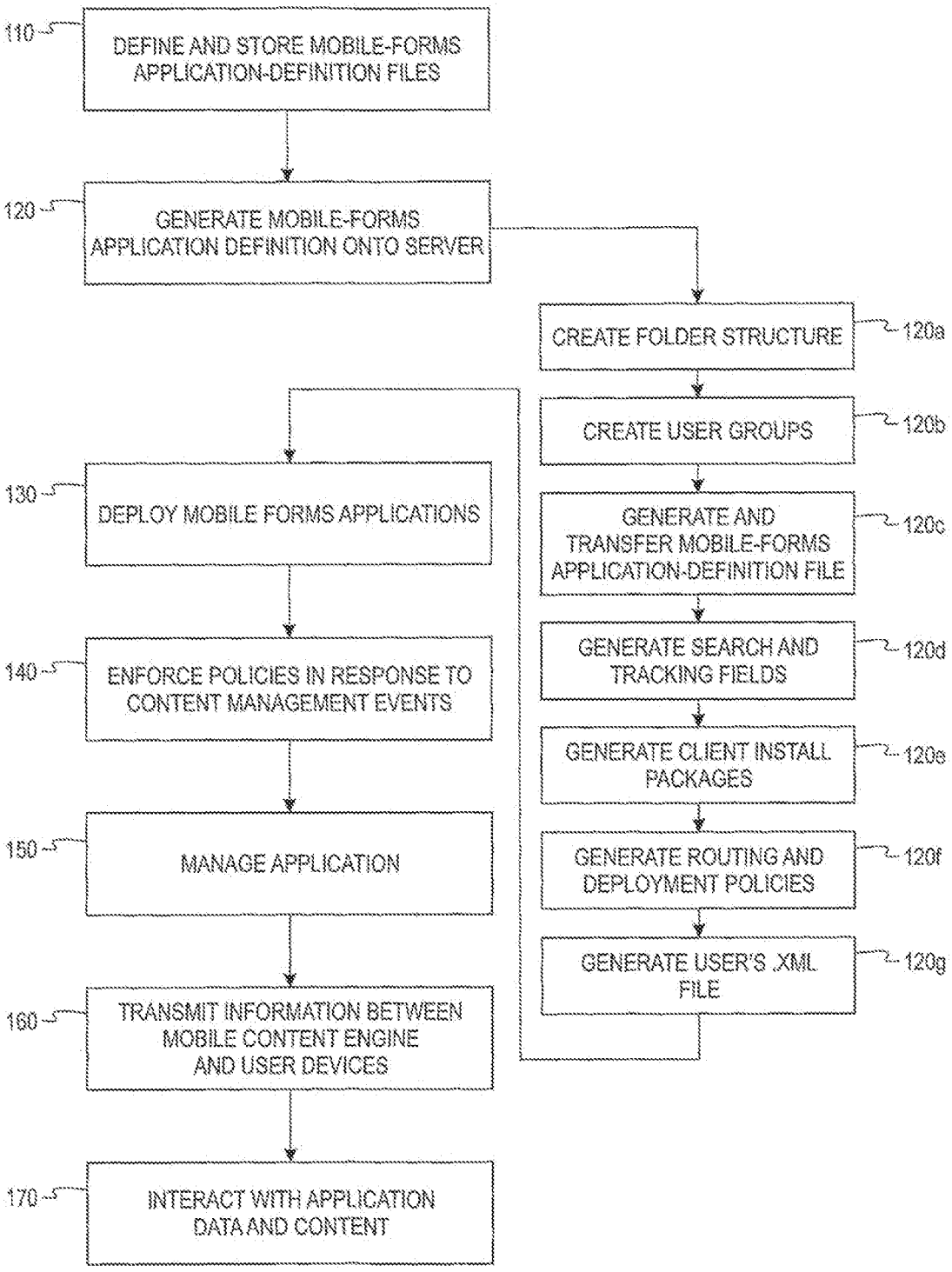

110
DEFINE AND STORE MOBILE-FORMS APPLICATION-DEFINITION FILES
120
GENERATE MOBILE-FORMS APPLICATION DEFINITION ONTO SERVER
CREATE FOLDER STRUCTURE
120a
CREATE USER GROUPS
120b
GENERATE AND TRANSFER MOBILE-FORMS APPLICATION-DEFINITION FILE
120c
GENERATE SEARCH AND TRACKING FIELDS
120d
GENERATE CLIENT INSTALL PACKAGES
120e
GENERATE ROUTING AND DEPLOYMENT POLICIES
120f
GENERATE USER'S .XML FILE
120g
130
DEPLOY MOBILE FORMS APPLICATIONS
140
ENFORCE POLICIES IN RESPONSE TO CONTENT MANAGEMENT EVENTS
150
MANAGE APPLICATION
160
TRANSMIT INFORMATION BETWEEN MOBILE CONTENT ENGINE AND USER DEVICES
170
INTERACT WITH APPLICATION DATA AND CONTENT

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2006/000076

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06Q 10/00*** (2006.01), ***H04L 12/16*** (2006.01), ***G06F 17/00*** (2006.01), ***G06K 9/78*** (2006.01), ***G06F 17/20*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: G06Q 10/00; H04L 12/16; G06F 17/00; G06K 9/78; G06F 17/20; (2006.01); G06F 17/00; IPC(7)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Canadian Patent Database, Google: mobile, wireless, form, document, application, definition file, extensible markup language, electronic/mobile form, paper, scan, template,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0194219 (Bradley et al.) 19 December 2002 (19-12-2002) see whole document	1-34
Y	US 2003/0220879 (Gaughan et al.) 27 November 2003 (27-11-2003) see whole document	1-30
Y	US 5,034,096 (Beizer) 01 October 1991 (01-10-1991) see whole document	31-34
A	WO 01/61517 (Buisman et al.) 23 August 2001 (23-08-2001) see whole document	31-34

[ ] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 June 2006 (02-06-2006)	12 June 2006 (12-06-2006)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Chaza Nasrallah (819) 934-2627

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2006/000076

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2002194219	19-12-2002	CA2344074 A1	17-10-2002
		CA2381832 A1	17-10-2002
US2003220879	27-11-2003	None	
US5094098	01-10-1991	AT155268T T	15-07-1997
		AU622946 B2	30-04-1992
		AU4502389 A	14-05-1990
		DE68928166D D1	14-08-1997
		DE68928166T T2	16-07-1998
		EP0400113 A1	05-12-1990
		ES2017051 A6	16-12-1990
		JP3504545T T	03-10-1991
		WO9004837 A1	03-05-1990
WO0161517	23-08-2001	AU3695501 A	27-08-2001
		AU3818701 A	27-08-2001
		US6867789 B1	15-03-2005
		US2004243641 A1	02-12-2004
		WO0161598 A1	23-08-2001

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
2 May 2008 (02.05.2008)

(10) International Publication Number
WO 2008/051379 A2

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2007/021795

(22) International Filing Date: 12 October 2007 (12.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/551,404 20 October 2006 (20.10.2006) US

(71) Applicant *(for all designated States except US)*: **VERIZON SERVICES CORP.** [US/US]; 1320 North Courthouse Road, Arlington, VA 22201 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **BALIA, Bimal, K.** [US/US]; 18902 Fountain Hills Drive, Germantown, MD 20874 (US).

(74) Agents: **O'NEILL, David** et al.; Verizon Legal Department, Patent Management Group, 1515 Courthouse Road, Suite 500, Arlington, VA 22201-2909 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: SYSTEM AND METHOD FOR MANAGING AND MONITORING MOBILE DATA, CONTENT, ACCESS AND USAGE

(57) Abstract: A system, method, and process for managing and monitoring mobile data, content, access, and usage of mobile devices are provided. The described exemplary system, method, and process provide an infrastructure for managing and monitoring various applications and services of mobile devices such as Internet access, voice, messaging, gaming, music, and video.

WO 2008/051379 A2

SYSTEM AND METHOD FOR MANAGING AND MONITORING MOBILE DATA, CONTENT, ACCESS, AND USAGE

BACKGROUND

As the Internet increased in popularity, parents became worried about the content of the websites that their children were accessing. Today, the increasing use of mobile devices (e.g., cell phones, PDAs, pagers, and similar devices) have only further enhanced this and similar apprehensions of parents. Because many mobile devices can provide easy access to an array of applications from almost any location at any time, it has become increasingly difficult for parents to manage and monitor the mobile data, content, access, and usage of their children on their mobile devices. For example, many mobile devices allow users to access numerous applications such as voice (e.g., phone and voicemail), messaging (e.g., SMS /MMS), Internet, gaming, music, and video. Typically, the access to these applications can be easily obtained with the touch of a button. Moreover, each member of a household might have more than one mobile device, which would even further complicate the situation of managing and controlling children's use of their mobile devices.

In the past few years, many efforts have been made to address customers' needs in using mobile devices, but none provides a full solution for the above-stated problem. For example, some service providers offer customers "pay-as-you-go" plans to control use of their mobile devices, where if a customer's prepaid balance falls below a certain threshold, the service provider directs the subscriber to purchase additional time. However, such "pay-as-you-go" plans have limited applicability in the context of prepaid services. Another example is for service providers to provide customers or subscribers with mobile devices, e.g., cell phones, that were made with configurable restrictions, pursuant to which the customers or subscribers can program and personalize the devices. For instance, a parent is able to login to a child's phone to apply usage and phone number restrictions on that particular phone. This solution, again, is restrictive because it requires manual configuration of each of the pre-selected types of mobile devices.

In addition, like many other efforts, this solution fails to address customers' concerns on the content accessible from the mobile devices.

In light of the above, there exists a need to provide customers, such as parents, with an improved comprehensive method and system for managing and monitoring the mobile data, content, access, and usage of their own or their affiliates' mobile devices.

BRIEF DESCRIPTION OF THE DRAWINGS

Reference will be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

Fig. 1 illustrates a system for managing and monitoring mobile data, content, access, and usage of mobile devices according to an embodiment.

Fig. 2 illustrates in further detail the components of the system in Fig. 1, including a service provider's network and a customer's access to the network according to an embodiment.

Fig. 3 shows a particular component in the system in Fig. 1, a Deep Inspection Application Control Server and primary application modules comprised thereof, according to an embodiment.

Fig. 4 is a flow chart showing the process algorithm performed by the system in Fig. 1 in managing and monitoring mobile data, content, access, and usage according to an embodiment.

DETAILED DESCRIPTION

Exemplary embodiments will now be described hereinafter with reference to the accompanying drawings, in which exemplary embodiments and examples are shown. Like numbers refer to like elements throughout.

Figs. 1 and 2 provide a high-level overview of an improved system for managing and monitoring mobile data, content, access, and usage of mobile devices according to one embodiment. As shown in Figs. 1 and 2, the management system **104** provides a network-based solution for managing and monitoring mobile data, content, access, and usage of mobile devices. Specifically, the management system **104** can be used to manage mobile data, content, access and usage of a user's mobile device **100** through a service provider's network **102**, or

the general Internet **120** or other wide area network where a service provider's online service applications can be accessed. Each of these components will be described in detail below with reference to Figs. 1 and 2.

As shown in Fig. 2, in operation, the management system **104** may involve a subscriber **122** and a user **124**. The subscriber **122** can be an entity (e.g., corporation) or an individual subscribing to mobile or wireless services from a mobile or wireless service provider (service provider), while a user **124** typically refers to an individual that operates a mobile device associated with a particular subscriber's **122** account. The mobile device operated by a user **124**, illustrated as the user's mobile device **100** in Figs. 1 and 2, can be a cellular phone, PDA, handheld, or any other portable computing device. Usually there is no limit to the number of subscribers **122** or users **124** associated with a specific account. For example, the subscriber **122** can be a parent and the users **124** may include all the children on the same subscribing account. In another instance, the subscriber **122** can be a corporation paying for the mobile or wireless services of its employees, and thus, all those beneficiary employees become the users **124**. On certain occasions, the subscriber **122** and user **124** can be the same entity, i.e., when the mobile service subscribing account has only one person associated therewith. Also, a user **124** may have more than one mobile device associated with an account subscribed to by the subscriber **122**. For instance, a parent may have both a cellular phone and a personal digital assistant (PDA) associated with the same account.

The service provider's network **102** illustrated in Figs. 1 and 2 can be any type of telecommunications networks. The service provider's network **102** may employ various protocols and technologies such as advanced mobile phone systems (AMPS), time division multiple access (TDMA), code division multiple access (CDMA), and global system for mobile communications (GSM). Many of these radio-based networks operate with base stations that initially handle the incoming traffic. The base station function is often divided into two main functional elements: the Base Station Controller (BSC) and the Base Transceiver System (BTS) **126**, as shown in Fig. 2. The BTS **126** consolidates several transceivers at a single location. The BTS **126** may communicate with and pass traffic to the Gateway GPRS Support Nodes (GGSN) **128** or Packet Data Serving

Nodes (PDSN) **128**. The GGSN **128** and PDSN **128** serve as gateways between mobile networks and packet data networks. Once the traffic reaches the service provider's network **102**, the service provider's network **102** can pass the traffic to the management system **104**.

In one embodiment, the management system **104** provides the subscriber **122** with significant control over a user's mobile device **100**, such as limiting the time duration of phone calls, time period of allowed calls, number of usable minutes in a particular time period, content of web-based applications, content and usage of multimedia applications, access to specific categories of videos and games, access to services that require a fee, access to specific websites, and numerous other applications. In another embodiment, the management system **104** is configured to provide a user-friendly programmable interface such that any service provider can integrate the system **104** into its existing systems and network **102** to allow its subscribers **122** to manage and monitor all traffic that passes to the user's mobile device **100**. Alternatively, the management system **104** can be separate from but accessible to a service provider's network **102**. The management system **104** according to an exemplary embodiment is not dependent upon the protocols or technologies employed in a particular service provider's network **102**. In addition, the applicability of management system **104** is not limited to the wireless or mobile context; instead, it can be seamlessly integrated into any wired network to perform similar management functionalities with respect to wireline devices.

Figs. 1 and 2 also provide an architectural view of the management system **104** of one embodiment. Typically, the management system **104** resides on a web server in a computer network, which can be a packet switched network, such as a wide area network (WAN), a local area network (LAN), metropolitan area network (MAN), the Internet, or any other similar types of communication networks. Various protocols can be utilized by these computer networks, including Internet Protocol (IP), Frame Relay (FR), Point-to-Point Protocol (PPP), or any other data protocol. Moreover, the computer network typically contains switching or routing equipment designed to transfer the traffic to different segments or components of the network. The network traffic may be of any type including text, graphics, video, e-mail, multimedia, documents, voice, audio, and any other forms of data.

In operation, the traffic would be passed to the management system **104** by the service provider's network **102**. The architecture of Figs. 1 and 2 is only exemplary and various embodiments can be used with any type of communications system, computer network, protocol, or combination thereof.

Referring to Figs. 1, 2, and 3, a detailed description of each component of the management system **104** according to various embodiments is provided. At a high level, in one embodiment, the management system **104** comprises a Web Account Access Portal **106**, Policy Authentication Server **108**, Policy Database **110**, Deep Inspection Application Control Server **112**, Subscriber Monitoring Device **114**, and Partner Web Portal **116**.

As shown in Figs. 1 and 2, the Web Account Access Portal **106** provides a subscriber **122** with an interface through which the subscriber **122** can manage and monitor the mobile devices associated with the subscriber's account. As such, the Web Account Access Portal **106** is generally embodied by software that is stored by a memory device, such as a server within the management system **104**, and that is configured to provide the interface for providing the subscriber with the requested information and for receiving input from the subscriber as described herein upon execution of the software, such as by a server or the like. The subscriber **122** can access the Web Account Access Portal **106** via a network, such as the Internet **120**, through a device capable of accessing the network, such as a mainframe station, a desktop PC, a laptop PC, a hand held device (e.g., PDA or data acquisition and storage device), or a processing device embodied within another apparatus. Through the network-accessible device, a subscriber **122** may login to the subscriber's account and, for each mobile device associated with the subscriber's account, establish a Policy Profile **111** in the Policy Database **110**. As shown in Figs. 1 and 2, one subscriber may have more than one policy profile **111** when there are multiple mobile devices associated with the subscriber's account. In operation, the subscriber **122** can associate, create, update, modify, delete, and store a Policy Profile **111** for each mobile device associated with the subscriber's account. Typically, a Policy Profile **111** is defined to include various parameters set forth by the subscriber **122** for a specific mobile device. For example, the subscriber **122** can configure the Policy Profile **111** to contain a time period where incoming calls are prohibited, an access limitation that only allows access to video

games with a PG or G rating, or a content limitation that only permits Internet access to educational websites. Through the Web Account Access Portal **106**, the subscriber **122** can also monitor various incoming requests from each user's mobile device **100**, due to, in large part, the ability of the management system **104** to track and provide statistics as well as almost real-time status regarding the data, content, access, and usage of each mobile device. For instance, a subscriber **122** can login to the Web Account Access Portal **106** and view how many minutes were used during a particular time period, what websites were accessed, what websites were attempted to be accessed but for which access was denied, and what types of games were played. In an exemplary embodiment, the Web Account Access Portal **106** is configured to access the Policy Database **110** and communicate with the Subscriber Monitoring Device **114** through a network, such as the Internet **120**. In addition, the Web Account Access Portal **106** may interact with the Partner Web Portal **116** through the service provider's private media intranet **118**, as will be described in detail below.

The Policy Authentication Server **108**, as illustrated in Figs. 1 and 2 is configured to access and retrieve data in the Policy Database **110**, to determine whether a user's mobile device **100** is associated with any Policy Profile **111**. If the Policy Authentication Server **108** identifies a Policy Profile **111** associated with the user's mobile device **110**, the Policy Authentication Server **108** will send instructions to the service provider's network **102** before allowing the traffic to be sent to the user's mobile device **100**, with the instructions specifying that the traffic directed to the user's mobile device **100** should be mirrored to the management system **104** for inspection prior to delivery to the user's mobile device **100**. In inspecting the mirrored traffic, the management system **104** would specifically examine whether the traffic complies with the Policy Profile **111** and then determine whether the traffic is allowed to reach the user's mobile device **100**. Alternatively, if the Policy Authentication Server **108** determines that a user's mobile device **100** is not associated with any Policy Profile **111**, the Policy Authentication Server **108** will instruct the service provider's network **102** to transmit the traffic to the user's mobile device **100** without mirroring the traffic to the management system **104**. In that scenario, the management system **104** does not need to inspect the traffic directed to a user's mobile device **100**. The Policy

Authentication Server **108** queries the Policy Database **110** to determine if a user's mobile device **100** has a Policy Profile **111** associated with it. These queries by the Policy Authentication Server **108** to the Policy Database **110** are generally executed based on information about a user's mobile device **100** contained in layer 2 or layer 3 of the packets (corresponding to the Open Systems Interconnection (OSI) Model) or, in the case of a phone, it can be based on the Mobile Subscriber ISDN (MSISDN) number, although other identifiers of the data packets may be employed.

The Policy Authentication Server **108** typically comprises a processor or other computing device (hereinafter generically referenced as a "processor") that is configured to be able to access to one or more databases stored in a secondary memory or primary memory. Usually the processor is also configured to communicate with external devices using an I/O controller that typically interfaces with a LAN. The memory and/or external devices may be integrated as part of the Policy Authentication Server **108**, or alternatively, reside in different, proximate or remote, locations that are accessible to the Server **108**. For example, the communication between the Server **108** and the remote devices is typically accomplished by routing data from the LAN over a communications facility to a WAN. One or more of the Policy Authentication Servers **108** may be used in exemplary embodiments.

In Figs. 1 and 2, only one Policy Database **110** is illustrated, but again, the Policy Database **110** may include several databases, each of which is configured to store various Policy Profiles **111**. In one embodiment, through various network connections, the data in the Policy Database **110** is made easily accessible to various components of the management system **104**, such as the Web Account Access Portal **106** as described above, the service provider's network **102**, the Policy Authentication Server **108**, and the Deep Inspection Application Control Server **112**.

As will be further illustrated in Fig. 3, the Deep Inspection Application Control Server **112** contains at least one inspection application **113** that is designed and configured to examine data directed to a specific user's mobile device **100** against the associated Policy Profile **111** to determine whether certain content and usage limitations as set forth in the Policy Profile **111** are satisfied. A typical

inspection process works as follows: upon the determination that a Policy Profile **111** is associated with a particular user's mobile device **100**, the Policy Authentication Server **108** will retrieve a copy of Policy Profile **111** from the Policy Database **110** and transmit the Policy Profile **111** to the Deep Inspection Application Control Server **112**. In response to the received data traffic and Policy Profile **111**, the Deep Inspection Application Control Server **112** will select and execute a particular inspection application **113** that is designed to inspect the data traffic against the Policy Profile **111**. If the traffic does not comply with the Policy Profile **111** associated with the user's mobile device **100**, the Deep Inspection Application Control Server **112** will then inform the Authentication Server **130** of the noncompliance. In response, the Authentication Server **130** would start several protective actions, including (1) providing a redirect message to the user's mobile device **100**, in the form of a text message to the mobile device that provides the customer service contact number of the service provider's network **102** that the user **100** can contact in order to identify the reason for the failure of a specific service request, (2) prohibiting the user's mobile device **100** from accessing to the requested service or application, and (3) updating the information in the Subscriber Monitoring Device **114**, such as the activity history of the user's mobile device **100** to record the access attempts and any denials. In practice, the traffic directed to a particular user's mobile device **100** may be identified by the Deep Inspection Application Control Server **112** and the inspection application **113** based on various identifiers, such as the MAC address (e.g., layer 2 information), the IP address (e.g., layer 3 information), the MSISDN number, or any other traffic identifiers.

The Deep Inspection Application Control Server **112** also typically comprises a processor or other computing device (hereinafter generically referenced as a "processor") that is configured to be able to access to one or more memory device. Usually the processor is also configured to communicate with external devices using an I/O controller that typically interfaces with a LAN. The memory and/or external devices may be integrated as part of the Deep Inspection Application Control Server **112**, or alternatively, reside in different, proximate or remote, locations that are accessible to the Server **112**. For example, the communication between the Server **112** and the remote devices is typically

accomplished by routing data from the LAN over a communications facility to a WAN. One or more of the Deep Inspection Application Control Servers **112** may be used in exemplary embodiments.

In another embodiment, the Deep Inspection Application Control Server **112** is also configured to transmit data (e.g., the content and usage statistics) regarding each user's mobile device **100** for updating the information in the Subscriber Monitoring Device **114**. As a result, a subscriber **122** is able to monitor the traffic of each user's mobile device **100** associated with the subscriber's **122** account. Reversely, the Deep Inspection Application Control Server **112** can query the Subscriber Monitoring Device **114** to obtain statistics and information regarding previous activity (e.g., the number of minutes used to date) of a user's mobile device **100**.

Depending on the specific inspection functions (i.e., what service parameters to inspect), more than one inspection application **113** may be implemented and stored on the Deep Inspection Application Control Server **112**. For example, Fig. 3 shows several exemplary inspection applications **113**, including, and not limited to, an application for inspecting the time duration permitted for a single call, an application for inspecting the time period of allowed calls, an application for inspecting the number of usable minutes in a particular time period, an application for inspecting the allowable content rating for web-based applications, an application for inspecting the allowable content rating for multimedia applications, an application for inspecting access to specific URLs, and an application for managing numerous other applications and services. As a person of ordinary skill may appreciate, in operation, the inspection application **113** may be varied, customized and implemented to tailor specific customer needs. In inspecting the traffic directed to a user's mobile device **100** for compliance with its Policy Profile **111**, the inspection application **113** typically examines whether certain pre-defined thresholds or requirements in the Policy Profile **111**, such as usage or content limitations, are satisfied in the inspected traffic.

The Subscriber Monitoring Device **114**, depicted in Figs. 1 and 2, is typically embodied by a computing device, such as a personal computer, operating under software control to enable a subscriber to track statistics as well as almost real-time information regarding the content, access, and usage of each mobile

device associated with a subscriber's account. In operation, the Subscriber Monitoring Device **114** receives statistical or real-time data from the Deep Inspection Application Control Server **112** and saves the received data in one or more databases that are accessible to other web servers and portals, such as the Web Account Access Portal **106** shown in Figs. 1 and 2. Through the communication between the Web Account Access Portal **106** and the database(s) associated with the Subscriber Monitoring Device **114**, a subscriber **122** may submit inquiries and receive answers about statistics as well as almost real-time information regarding the content, access, and usage of each mobile device associated with the subscriber's account. Alternatively, the data in those database(s) associated with the Subscriber Monitoring Device **114** can be uploaded to the Web Account Access Portal **106** for a subscriber **122** to search and view. For instance, a subscriber **122** can view the number of minutes used during a particular time period, the websites accessed, the websites to which access was denied and the games played.

Figs. 1 and 2 also illustrate a Partner Web Portal **116** that provides an interface through which a service provider may provide its users with easy access to a series of media services, such as video, music, entertainment, and games for a fee or on a complimentary basis. In practice, the Partner Web Portal **116** is generally embodied by software that is stored by a memory device and that is configured to provide the aforementioned interface upon its execution, such as by a media server that is configured to provide services such as video, music, entertainment, and games to a user's mobile device **100**. In one embodiment, the media server of the Partner Web Portal **116** is configured to be connected to a service provider's private media intranet **118**, and further, to the service provider's network **102**. Under this configuration, the media server of the Partner Web Portal **116** is able to communicate with various web servers and portals such as the Web Account Access Portal **106**. As a result, a subscriber **122** is able to, by logging onto the Web Account Access Portal **106**, pre-define and configure what media services and applications can be allowed for each user's mobile device **100** associated with the subscriber's account. For future inspection purposes, such pre-definition and configuration is to be stored in the Policy Profile **111** associated with the user's mobile device **100**.

The management system **104** is capable of managing and monitoring the mobile data, content, access, usage and other information concerning different users' mobile devices associated with a subscriber's account. For further illustration of the system's functionalities, the following exemplary services and applications will be described.

In one embodiment, the management system **104** can manage and monitor the duration of phone calls or other services and applications. For example, a subscriber **122** can configure the Policy Profile **111** associated with a user's mobile device **100** to limit the duration of phone calls, games, or Internet access to two minutes per session during a specified time period, e.g., from 12:30 PM to 6:00 AM. By setting such time limitations, the subscriber **122** may discourage unnecessary lengthy use of phone services, especially during an expected busy time period. This service can be monitored by the management system **104** that performs a process of inspecting layer 2 or layer 3 of data packets. Specifically, time stamps on the data packets would be examined to determine whether a call exceeds the time duration as defined in the Policy Profile **111**. If so, the active call will be inactivated or terminated, preferably, with a warning message to the user.

In another embodiment, the management system **104** provides a scheduling function that allows a subscriber **122** to set a time period where access to the Internet, games, music, or incoming phone calls should be denied on a user's mobile device **100**. For example, through this scheduler function, parents can set the time limitation, e.g., between 12:30 PM and 6:00 AM, to their children's use of mobile devices. In operation, a subscriber **122** includes the time limitation in the Policy Profile **111**. When the data packets are received, the management system **104** would first inspect the time stamps at layer 2 or layer 3 of the data packets or the MSISDN number of each incoming phone call, then verify the time information with the control settings in the Policy Profile **111**, and finally decide whether to block or allow the data session. However if a call is being received by or originated from numbers within the subscriber's account, these calls will be permitted.

Moreover, the management system **104** can provide the subscriber **122** with the ability to set usage limits on various applications and services. For example, the subscriber **122** can limit the number of MMS/SMS messages or picture

messages to 175 messages for a specific time period. Because the Subscriber Monitoring Device **114** tracks statistics regarding the data, content, access, and usage of each mobile device, the Deep Inspection Application Control Server **112** can send queries to the Subscriber Monitoring Device **114** to obtain the statistics and information regarding previous activity, e.g., the total number of messages sent during the specified period. As a result, the Deep Inspection Application Control Server **112** can enforce the messaging limitation contained in the Policy Profile **111** with accuracy.

The management system **104** can also provide a subscriber **122** with the ability to control users' access to various web-based applications from their mobile devices. With the increasing access to the Internet from mobile devices, such capability has become significantly useful, especially for parents to prevent their children from accessing or downloading specific categories of videos and games. In one exemplary embodiment, the management system **104** can monitor and prevent access to specific websites by, for example, searching for key words within the text, image names, or URL of each webpage. Alternatively, the Partner Web Portal **116** is configured to allow the management system **104** to prevent certain applications and services from reaching a user's mobile device **100**. Under this alternative configuration, the service provider can assign each service and application (e.g., games, videos, music, chat rooms, and media based applications) a rating. For example, each service or application could be assigned a rating such as G, PG, Y7, R15, R18, R21, and XXX. Using the rating information, a subscriber **122** can set the allowable rating level for each mobile device and prevent access to any applications or services on the Partner Web Portal **116** that fall below the allowed rating for the user **124**. As stated above, all the restrictions to the web related content, access, usage of a user's mobile device will be pre-defined and stored in the Policy Profile **111** associated with the user's mobile device.

The services and functions provided by the management system **104** are not limited to the above-illustrated examples. Instead, many alternative applications and services may be offered according to various exemplary embodiments.

Referring to Fig. 4, an exemplary process performed by the management system **104** in monitoring, controlling and managing data, content, usage of users'

mobile devices will be described. For easy illustration, a parent-child scenario is used in the following process, but embodiments are not limited to the illustration, and can apply in various other contexts where mobile phone use needs to be monitored.

Before the process begins, a parent establishes an account with a service provider for wireless or mobile services. The parent further establishes his child as a user **124** on the account. Thus, the parent is now a subscriber **122**, and his child is now a user **124**. The subscriber **122** is provided with credentials (i.e., user name and password) to obtain access to the Web Account Access Portal **106**.

As shown in Step **136**, the subscriber **122** logs onto the Web Account Access Portal **106** to define various controls for his child's **124** mobile device ("user's mobile device **100**"), e.g., usage, duration, scheduling, application-based activities, and multimedia applications. Such pre-defined controlling information will be saved in a Policy Profile **111** that is associated with the user's mobile device **100** in the Policy Database **110**. The Policy Profile **111** can be updated whenever the subscriber **122** changes the control instructions on the use of users' mobile devices associated with the subscriber's account, as shown in Step **138**.

When the user **124** needs to use a service or application that requires access to the service provider's network **102** and attempts to initiate a data session, in Step **140**, the user's mobile device **100** originates a data session request with the service provider's network **102**. In Step **142**, the Authentication Server **130** receives an authentication message from the GGSN/PDSN **128** to have the user's mobile device **100** authenticated before permitting the data session setup. Then in Step **144**, the Authentication Server **130** determines the authenticity of the user's mobile device **100** by sending queries to the Sub Policy Database **132** to determine whether the user's mobile device **100** is valid or registered. If the user's mobile device **100** is valid or registered, the Authentication Server **130** will send a request to the Policy Authentication Server **108** to identify whether a Policy Profile **111** is associated with the user's mobile device **100** as shown in Step **146**.

In Step **148a**, if no Policy Profile **111** is associated with the user's mobile device **100**, the Authentication Server **130** will instruct the service provider's network **102** to transmit the data from the High Speed Gateway/Router **134** to the user's mobile device **100** without any additional inspection by the Deep Inspection

Application Control Server **112**. Alternatively, if the user's mobile device **100** is associated with a Policy Profile **111**, the Authentication Server **130** will instruct the High Speed Gateway/Router **134** to mirror the traffic directed to the user's mobile device **100** to the Deep Inspection Application Control Server **112** for inspection before passing the data packets to the user's mobile device **100** in Step **148b**. In this regard, the management system **104** would permit the service provider's network **102** to transmit data from the High Speed Gateway/Router **134** to the user's mobile device **100** if it complies with the Policy Profile **111**.

In preparation for performance of the inspection, the Deep Inspection Application Control Server **112** may be updated in Step **150** in accordance with the Policy Database **110** to reflect any updates in the Policy Profile **111** associated with the user's mobile device **100**. In Step **154**, the High Speed Gateway/Router **134** inspects all data packets and mirrors the packets tied to a Policy Profile **111** to the Deep Inspection Application Control Server **112** based on the IP address of the user's mobile device **100**. If the user's mobile device **100** does not have a Policy Profile **111** associated with it, its traffic passes from the High Speed Gateway/Router **134** without inspection by the management system **104** as noted above.

In response to receiving packets tied to a Policy Profile **111**, specific categories of the inspection applications **113** that are available to the Deep Inspection Application Control Server **112** that are to be controlled in the Policy Profile **111** would be triggered and executed by the Deep Inspection Application Control Server **112** in Step **160**. In Step **162**, based on the IP addresses, the activated inspection applications **113** inspect the traffic for usage and content compliance with the Policy Profile **111** associated with the user's mobile device **100**. Depending on the application or service, this inspection can be done from layer 2 to layer 7. If the traffic does not comply with the Policy Profile **111**, the Deep Inspection Application Control Server **112** signals the Authentication Server **130**, and in response, the Authentication Server **130** will, as shown in Step **164**, perform an authentication process, including the steps of: (1) providing a redirect message to the user's mobile device **100**, (2) preventing access to the requested site, games portal, videos, etc., and (3) sending updates to the Subscriber Monitoring Device **114** to update the activity history for the user's mobile

device **100**. In Step **166**, the Subscriber Monitoring Device **114** tracks the activity statistics of each user's mobile device **100** based on updates from the Deep Inspection Application Control Server **112**. In Step **168**, the Subscriber Monitoring Device **114** will send updates on the activity statistics to the Web Account Access Portal **106** so that the subscriber **122** may view the status of users' mobile devices in almost real time.

As described above, exemplary embodiments may take the form of a computer program product on a computer-readable storage medium having computer-readable program instructions (e.g., computer software) embodied in the storage medium. Any suitable computer-readable storage medium may be utilized including hard disks, CD-ROMs, optical storage devices, or magnetic storage devices.

Exemplary embodiments have been described above with reference to block diagrams and a flowchart illustrations of methods, apparatuses (i.e., systems) and computer program products. It will be understood that each block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by various means including computer program instructions. These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus create a means for implementing the functions specified in the flowchart block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including computer-readable instructions for implementing the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the

instructions that execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

In the preceding specification, various embodiments of the claimed invention have been described. It will, however, be evident that various modifications and changes may be made thereunto without departing from the broader spirit and scope of the invention as set forth in the claims that follow. The specification and drawings are accordingly to be regarded in an illustrative rather than restrictive sense.

THAT WHICH IS CLAIMED:

1. A system comprising:

a web account access portal that provides an interface to a subscriber enabling the subscriber to configure a policy profile for association with at least one mobile device;

a policy profile database that contains at least one policy profile associated with at least one mobile device; and

a deep inspection application control server that includes at least one inspection application that inspects data requested from a user's mobile device for compliance with the policy profile associated with the user's mobile device.

2. The system of claim 1 wherein the web account access portal updates the policy profile database with a policy profile associated with a user's mobile device according to the configuration set by the subscriber.

3. The system of claim 1 further comprising:

a subscriber monitoring device wherein the deep inspection application control server updates the subscriber monitoring device with information regarding the data requested from the user's mobile device.

4. The system of claim 3 wherein the subscriber monitoring device records information about the data requested by a user's mobile device and further allows a subscriber to view this information through the web account access portal via a interface

5. The system of claim 1 further comprising:

a partner web portal that is provided by a service provider from the service provider's own network wherein the partner web portal includes at least one media server from which a user's mobile device may request services according to the policy profile associated with the user's mobile device.

6. The system of claim 1 further comprising:

a policy authentication server that is enabled to make requests to the policy profile database to have the policy profile database determine if a policy profile is associated with a user's mobile device and wherein the policy authentication server is further operable to take action in response to the replies received from the policy profile database.

7. A process comprising:

receiving a data request from a user's mobile device;

determining if the user's mobile device has an associated policy profile; and

in response to determining that the user's mobile device has a policy profile associated with it, sending a copy of the data directed to the user's mobile device to an inspection application for inspection of the data according to the policy profile and only allowing the data complying with the policy profile to be sent the user's mobile device.

8. The process of claim 7 further comprising, in response to determining that the user's mobile device does not have a policy profile associated with it, allowing all data requested by the user's mobile device to be transmitted to the user's mobile device without inspecting the data.

9. The process of claim 7 further comprising:

providing a web account access portal to a subscriber via a interface wherein a subscriber can configure a policy profile and associate the policy profile with a user's mobile device.

10. The process of claim 9 wherein the web account access portal includes sending a request to a policy profile database to store the policy profile configured by a subscriber.

11. The process of claim 7 further comprising:

selecting one or more inspection applications to be associated with the user's mobile device based upon the associated policy profile; and

examining the data sent to a user's mobile device in accordance with the selected inspection application(s) for compliance with the policy profile associated with the user's mobile device and only allowing the data complying with the policy profile to be sent the user's mobile device.

12. The process of claim 11 wherein examining the data includes sending a message to the user's mobile device if the selected inspection applications determine that the data does not comply with the policy profile associated with the user's mobile device and preventing access to the data if the data does not comply with the policy profile associated with the user's mobile device.

13. The process of claim 7 further comprising:

monitoring the data requests from the user's mobile device; and

recording the information about the data requested from the user's mobile device.

14. The process of claim 13 further comprising providing information about the data requested from the user's mobile device to a portal for viewing by a subscriber.

15. A computer program product comprising a computer-readable storage medium having computer-readable instructions stored therein, the computer-readable instructions comprising:

first instructions configured to allow a user to configure a policy profile and associate the policy profile with a user's mobile device;

second instructions configured to store the policy profile;

third instructions configured to receive a request for data from a user's mobile device;

fourth instructions configured to determine if the user's mobile device has an associated policy profile; and

fifth instructions configured, in response to a determination that the user's mobile device has an associated policy profile, to send a copy of the data to an inspection application for inspection of the data according to the policy profile and

only allowing the data that complies with the policy profile to be sent to the user's mobile device; and

16. The computer program product of claim 15 further comprising sixth instructions configured, in response to a determination that the user's mobile device does not have a policy profile associated with user's mobile device, to allow all data to pass to the user's mobile device without inspecting the data.

17. The computer program product of claim 15 further comprising sixth instructions configured to send a message to the user's mobile device if the data request does not comply with the policy profile associated with the user's mobile device.

18. The computer program product of claim 15 further comprising:

sixth instructions configured to select one or more inspection applications to be associated with the user's mobile device based upon the associated policy profile; and

seventh instructions configured to examine the data sent to a user's mobile device in accordance with the selected inspection application(s) for compliance with the policy profile associated with the user's mobile device and to only allow the data complying with the policy profile to be sent the user's mobile device.

19. An apparatus comprising:

a server configured to receive a data request from a user's mobile device, said server comprising a processor configured to:

determine if the user's mobile device has an associated policy profile;

send a copy of the data directed to the user's mobile device to an inspection application for inspection of the data according to the policy profile; and

only allow the data complying with the policy profile to be sent the user's mobile device in response to determining that the user's mobile device has a policy profile associated with it.

20. The apparatus of claim 19 wherein the processor is further configured, in response to determining that the user's mobile device does not have a policy profile associated with it, to allow all data requested by the user's mobile device to be transmitted to the user's mobile device without inspecting the data.

21. The apparatus of claim 19 wherein the processor is further configured to:
monitor the data requests from the user's mobile device; and
record the information about the data requested from the user's mobile device.

22. The apparatus of claim 21 wherein the processor is further configured to provide information about the data requested from the user's mobile device to a portal for viewing by a subscriber.

Fig. 1

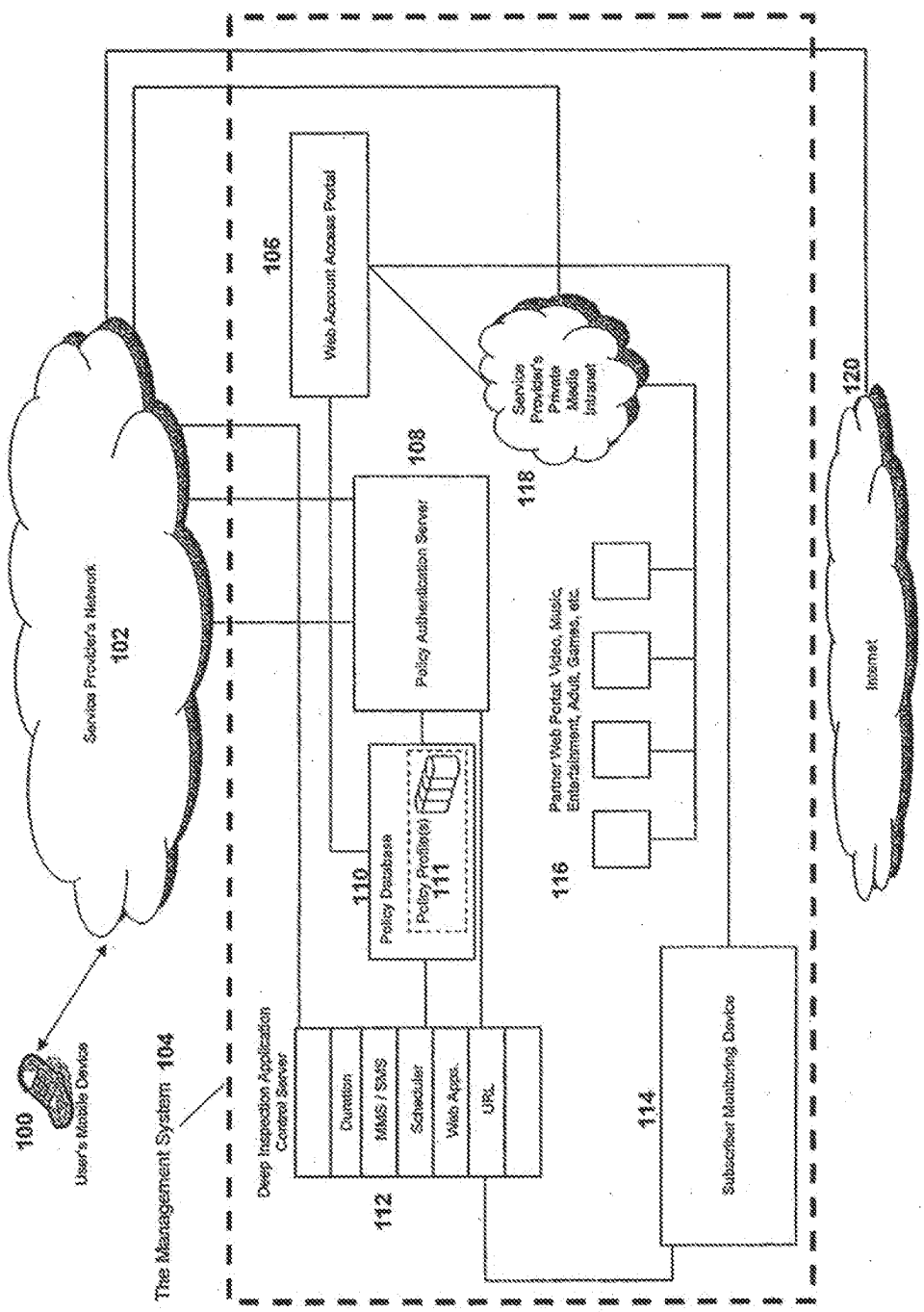

The Management System 104
Service Provider's Network
102
User's Mobile Device
100
Deep Inspection Application Control Server
Duration
MMS / SMS
Scheduler
Web Apps
URL
112
Policy Database
Policy Profile(s)
111
110
Policy Authentication Server
108
Web Account Access Portal
106
Service Provider's Private Media Intranet
118
Partner Web Portal: Video, Music, Entertainment, Adult, Games, etc.
116
Subscriber Monitoring Device
114
Internet
120

Fig. 2

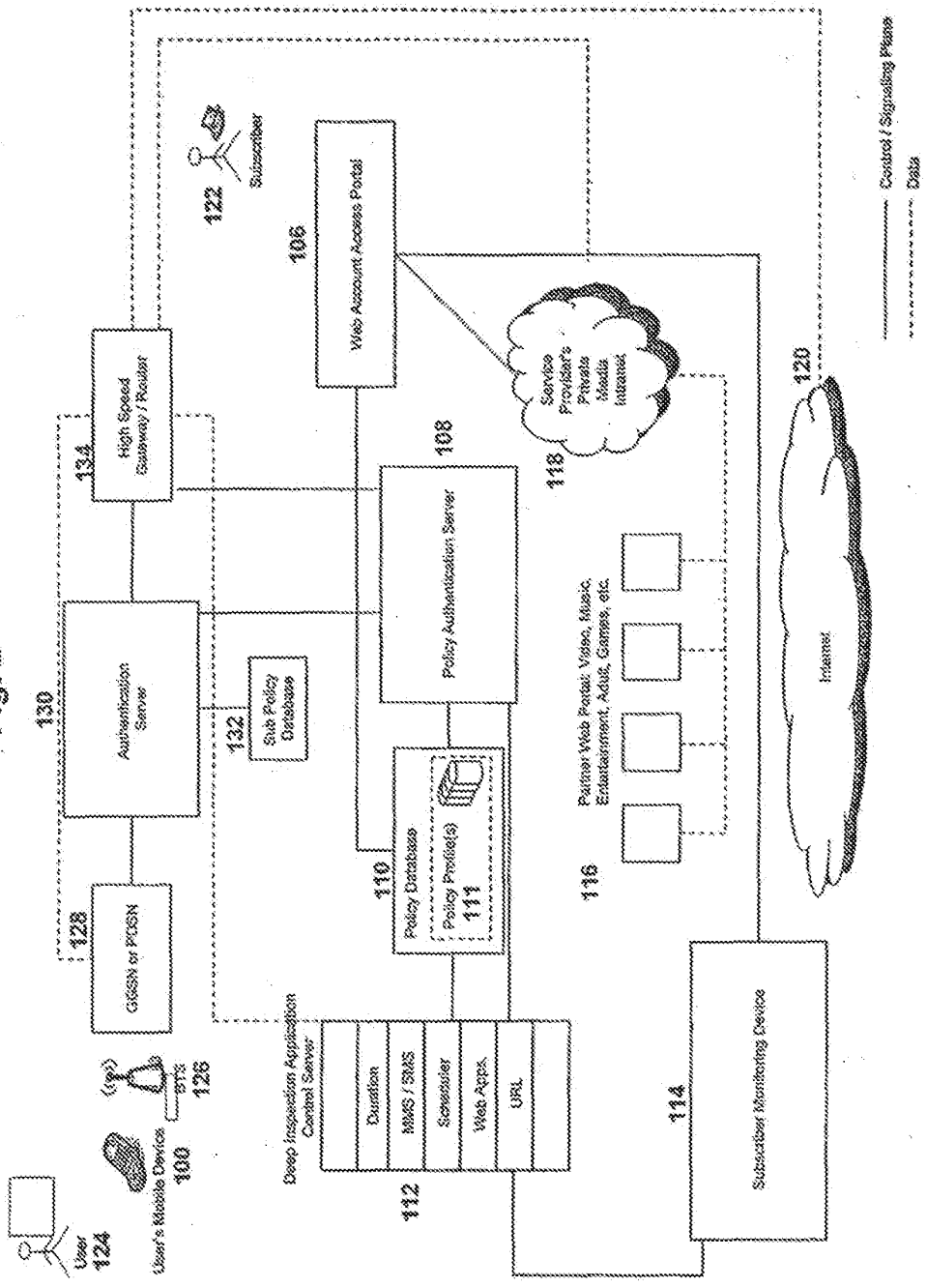

Control / Signaling Plane
Data
Subscriber
122
Web Account Access Portal
106
High Speed Gateway / Router
134
Service Provider's Private Media Internet
118
120
Internet
Policy Authentication Server
108
Authentication Server
130
Sub Policy Database
132
Policy Database
110
Policy Profile(s)
111
Partner Web Portal: Video, Music, Entertainment, Adult, Games, etc.
116
GGSN or PDSN
128
Deep Inspection Application Control Server
Duration
MMS / SMS
Screensaver
Web Apps
URL
112
Subscriber Monitoring Device
114
User
124
User's Mobile Device
100
126

Fig. 3

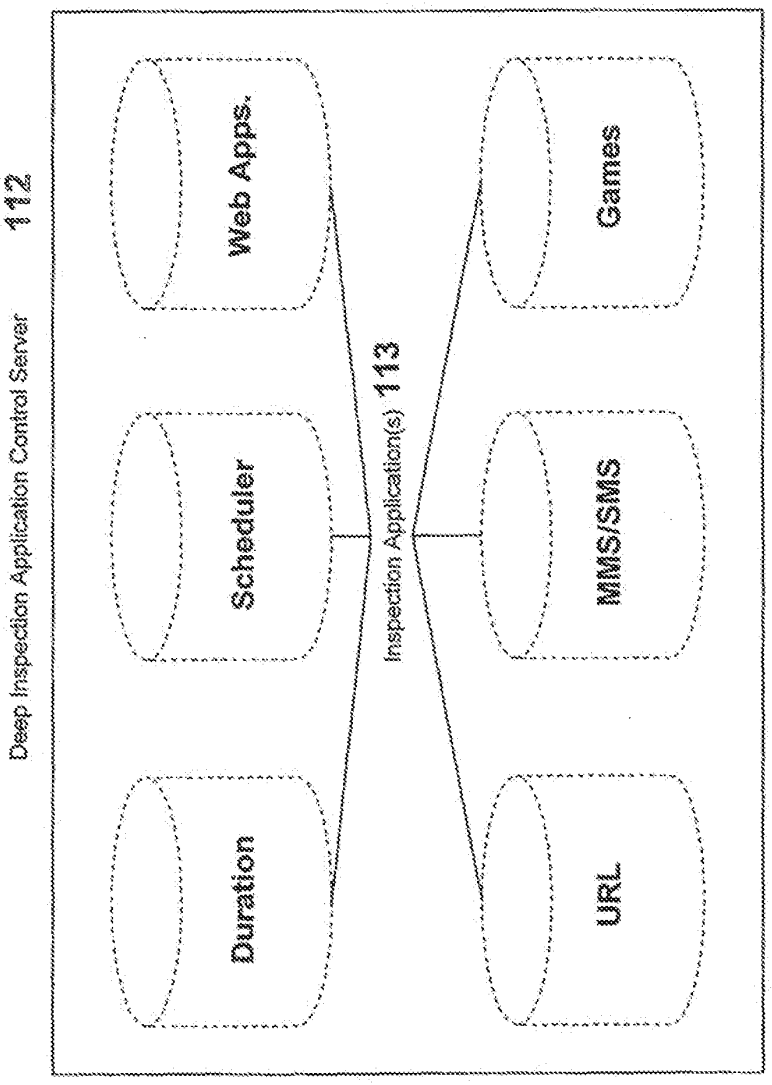
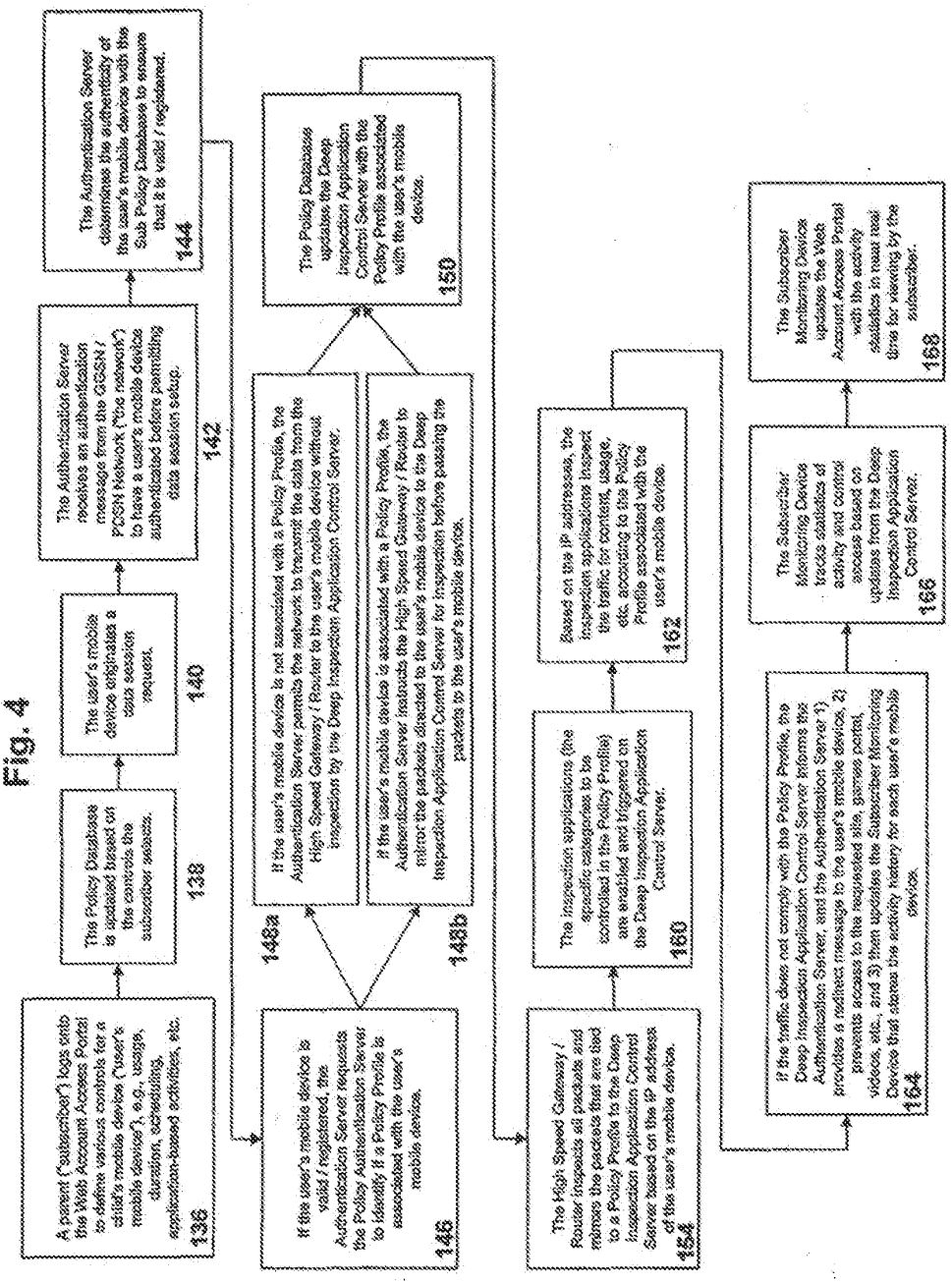

Deep Inspection Application Control Server 112
Inspection Application(s) 113
Web Apps.
Scheduler
Duration
Games
MMS/SMS
URL

Fig. 4


A parent ("subscriber") logs into the Web Account Access Portal to define various controls for a child's mobile device ("user's mobile device"), e.g., usage, duration, scheduling, application-based activities, etc.
136
The Policy Database is updated based on the controls the subscriber selects.
138
The user's mobile device originates a data session request.
140
The Authentication Server receives an authentication message from the GGSN / PDSN Network ("the network") to have a user's mobile device authenticated before permitting data session setup.
142
The Authentication Server determines the authenticity of the user's mobile device with the Sub Policy Database to assure that it is valid / registered.
144
If the user's mobile device is not associated with a Policy Profile, the Authentication Server permits the network to transmit the data from the High Speed Gateway / Router to the user's mobile device without inspection by the Deep Inspection Application Control Server.
148a
If the user's mobile device is associated with a Policy Profile, the Authentication Server instructs the High Speed Gateway / Router to mirror the packets directed to the user's mobile device to the Deep Inspection Application Control Server for inspection before passing the packets to the user's mobile device.
148b
The Policy Database updates the Deep Inspection Application Control Server with the Policy Profile associated with the user's mobile device.
150
If the user's mobile device is valid / registered, the Authentication Server requests the Policy Authentication Server to identify if a Policy Profile is associated with the user's mobile device.
146
The High Speed Gateway / Router inspects all packets and mirrors the packets that are tied to a Policy Profile to the Deep Inspection Application Control Server based on the IP address of the user's mobile device.
154
The inspection applications (the specific categories to be controlled in the Policy Profile) are enabled and triggered on the Deep Inspection Application Control Server.
160
Based on the IP addresses, the inspection applications inspect the traffic for content, usage, etc. according to the Policy Profile associated with the user's mobile device.
162
If the traffic does not comply with the Policy Profile, the Deep Inspection Application Control Server informs the Authentication Server, and the Authentication Server 1) provides a redirect message to the user's mobile device, 2) prevents access to the requested site, games portal, videos, etc., and 3) then updates the Subscriber Monitoring Device that stores the activity history for each user's mobile device.
164
The Subscriber Monitoring Device tracks statistics of activity and control access based on updates from the Deep Inspection Application Control Server.
166
The Subscriber Monitoring Device updates the Web Account Access Portal with the activity statistics in near real time for viewing by the subscriber.
168

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 July 2008 (03.07.2008)

PCT

(10) International Publication Number
WO 2008/080139 A1

(51) International Patent Classification:
H04J 3/14 (2006.01)

(21) International Application Number:
PCT/US2007/088732

(22) International Filing Date:
21 December 2007 (21.12.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/871,653 22 December 2006 (22.12.2006) US

(71) Applicant *(for all designated States except US)*: **INTEGRATED MOBILE, INC.** [US/US]; 8858 Commerce Loop Drive, Columbus, OH 43240 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PUGH, Greg** [US/US]; 379 Meditation Lane, Columbus, OH 43235 (US). **COLES, Sarah** [US/US]; 224 West Main Street, Mount Sterling, OH 43143 (US). **SLAWINSKI, Rick** [US/US]; 2590 Summit Street, Columbus, OH 43202 (US). **FISHER, Jason** [US/US]; 227 Bristol Drive, Delaware, OH 43015 (US). **NANKIVELL, Will** [US/US]; 6179 Brookmead Circle, Grove City, OH 43123 (US). **OLIVER, Erica** [US/US]; 485 McAlpin Avenue, Cincinnati, OH 43015 (US).

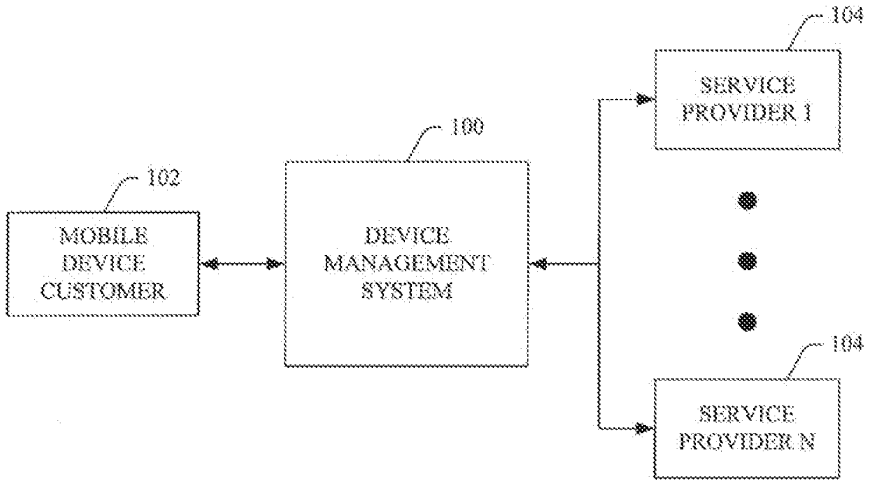
(74) Agents: **DORTENZO, Megan D.** et al.; Thompson Hine LLP, 127 Public Square, 3900 Key Center, Cleveland, OH 44114 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR MANAGING MOBILE DEVICES AND SERVICES



(57) Abstract: The mobile device management system provides for administration of mobile devices associated with a customer and supported by multiple service providers or carriers. The system provides a central, customized interface for management of mobile devices. The system aggregates customer policies, service plan information from various service providers and specific end user information to enable management of mobile devices. Management functions include procurement, expense management, billing and invoicing, support and monitoring of mobile devices associated with the customer. This system and method for managing mobile devices and services keeps the customers mobile workforce connected while reducing the total cost of ownership.

WO 2008/080139 A1

PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

BACKGROUND OF THE INVENTION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. provisional Application Serial No. 60/871,653, entitled, "System and Method for Managing Mobile Devices and Services," filed on December 22, 2006.

RELATED ART

[0002] Mobile communications and wireless connectivity are affordable to the vast majority of the population. Mobile devices have become an essential, ubiquitous element of today's business environment. Customers expect to be able to quickly reach the person they are calling, even when that person is not, for example, at their desk. Employers rely on being able to communicate with their employees at all times during the work day and often outside of traditional business hours as well.

[0003] Many companies therefore provide cell phones or wireless devices to their employees as part of their employment package. However, the large number of cell phone service providers, the myriad of service offerings and package deals now available, and the constant stream of new wireless devices coming from cell phone manufacturers have made it increasingly difficult for companies to do this effectively. As used herein, the term "service provider" refers to an entity or organization that provides support for mobile devices, such as a wireless carrier that operates a network for mobile phones.

[0004] More often than not, there is not a single mobile device and service plan that would serve all employees adequately. Rather, individual employees have widely varying needs based upon their individual job requirements and personal preferences. One employee may require only a basic cell phone. Other employees may require PDAs, wirelessly

equipped laptops, pagers, or combinations of devices depending on their individual needs. Some companies have employees that travel internationally and therefore it might be in the company's best interest to use a service provider whose network is compatible with the International GSM standard. Other companies might save money by forgoing international or nationwide coverage and use only a local reseller's network.

[0005] For budgetary reasons, employers often restrict employees to a particular subset of phones, such as those provided free with service plan commitments. Employees pay extra to upgrade to an enhanced phone with a camera, mp3 player, or other desired feature. For network compatibility reasons, employees may be restricted to certain service providers or phones, for example those compatible with the company's Good Technology® or Microsoft Exchange® email platforms.

[0006] Employees differ in their typical usage patterns. Some employees require only a simple voice plan, while others may require a data plan, text messaging, or even push-to-talk capability. A company can purchase bulk minutes to be shared among employees, or it may be more cost effective to purchase individual plans with a larger number of minutes and unlimited data usage for designated high usage employees. Billing is also an important consideration, as offices and business units may require individualized billing for employees in their groups. Breaking apart bills or inflexible billing that does not allow employees to easily move from one group to another as they are promoted or transferred can create unnecessary financial difficulties. Consequently, management of mobile devices, service plans and related issues quickly becomes a complex, costly, and time-consuming issue for many organizations.

SUMMARY

[0007] The following summary is intended to provide a simple overview as well as to provide a basic understanding of the subject matter described herein. It is not intended to describe or limit the scope of the claimed subject matter. Furthermore, this summary is not intended to describe critical or key elements of the claimed subject matter. Additional aspects and embodiments are described below in the detailed description.

[0008] The subject matter described herein is directed to methods and systems for facilitating mobile device management. The device management system provides for centralized administration of mobile devices for a mobile device customer. In particular, the

system provides for managing large numbers of mobile devices supported by multiple service providers with varying service plans. Service provider data, such as available service plans, devices, offers, discounts, and the like, is utilized in conjunction with customer data to manage procurement, allocation, distribution, support and/or billing for mobile devices for mobile device customers and end users of the mobile devices.

[0009] In certain embodiments, the system includes a procurement component that obtains mobile devices from a plurality of service providers in accordance with customer policies. In particular, end users utilize a customizable user interface to place orders and track shipment of mobile devices. In another embodiment, the procurement component complies with customer approval processes, obtaining appropriate authorizations prior to procurement of mobile devices.

[00010] In other embodiments, the device management system includes a billing component that aggregates invoicing and usage information from multiple service providers and allocates costs in accordance with customer policies. In an embodiment, costs are allocated based upon customer business unit. In another embodiment, costs are allocated both to the customer and to individual users as a function of service plan or function.

BRIEF DESCRIPTION OF THE DRAWINGS

[00011] The claimed subject matter is described with reference to the accompanying drawings. In the drawings, like reference numbers indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number identifies the drawing in which the reference number first appears.

[00012] FIG. 1 is block diagram of a system that manages mobile devices in accordance with an aspect of the subject matter described herein.

[00013] FIG. 2 is a block diagram of another embodiment of a system that manages mobile devices in accordance with an aspect of the subject matter described herein.

[00014] FIG. 3 is a block diagram of another embodiment of a system that manages mobile devices illustrating system inputs and output in accordance with an aspect of the subject matter described herein.

[00015] FIG. 4 is a detailed block diagram of the procurement component in accordance with an aspect of the subject matter described herein.

[00016] FIG. 5 is an exemplary methodology for managing a mobile device orders in accordance with an aspect of the subject matter described herein.

[00017] FIG. 6 is an exemplary methodology for updating the asset data store in accordance with an aspect of the subject matter described herein.

[00018] FIG. 7 is a detailed block diagram of an exemplary asset component in accordance with an aspect of the subject matter described herein.

[00019] FIG. 8 is an exemplary methodology for optimizing mobile device management in accordance with an aspect of the subject matter described herein.

[00020] FIG. 9 is an exemplary methodology for optimizing mobile device management in accordance with an aspect of the subject matter described herein.

[00021] FIG. 10 is a detailed block diagram of an exemplary support component in accordance with an aspect of the subject matter described herein.

[00022] FIG. 11 is a flowchart illustrating an exemplary methodology for providing support for mobile devices in accordance with an aspect of the subject matter described herein.

[00023] FIG. 12 is a flowchart illustrating an exemplary methodology for monitoring support in accordance with an aspect of the subject matter described herein.

[00024] FIG. 13 is a detailed block diagram of an exemplary billing component in accordance with an aspect of the subject matter described herein.

[00025] FIG. 14 is a flowchart depicting an exemplary methodology for transforming service provider information in accordance with an aspect of the subject matter described herein.

[00026] FIG. 15 is a flowchart depicting an exemplary methodology for processing service provider invoices in accordance with an aspect of the subject matter described herein.

[00027] FIG. 16 is a flowchart that depicts an exemplary methodology for configuring the device management system for a customer in accordance with an aspect of the subject matter described herein.

[00028] FIG. 17 is a flowchart depicting an exemplary methodology for configuring the user interface for a customer in accordance with an aspect of the subject matter described herein.

DETAILED DESCRIPTION

[00029] As described above managing mobile devices is a complex problem for many organizations. Service providers typically offer multiple service plans and device options, which vary in the type of services provided, usage rates, coverage areas, device requirements and capabilities, and other features. Large organizations or organizations with diverse needs may select multiple service plans offered by one or more carriers in order to meet the needs of its employee end users. In particular, an organization may elect to utilize multiple carriers, selecting different carriers for distinct regional offices, for individual functions, based upon user preference, corporate Information Technology (IT) policy, or any other criteria. Additionally, organizations frequently offer a specific set of paid services for one category of employees, agents, or other persons or entities designated to receive mobile devices and services (*e.g.*, technical support, upper level management or sales people), collectively referred to as end users, but offer more limited services to other categories of end users. Management of mobile devices, service plans and related issues quickly becomes a complex, costly, and time-consuming issue for organizations.

[00030] Turning now to FIG. 1, an exemplary device management system 100 that provides for centralized administration of mobile devices for one or more customers 102 is illustrated. As used herein, the term "exemplary" indicates a sample or example. It is not indicative of preference over other aspects or embodiments. The term "mobile device" refers to cellular phone, PDA, laptop, wireless data card, smart phone, or any other device capable of wireless communication. Also, as used herein, the term "customer" indicates an entity, business, organization or other logical group of mobile device end users. In addition, the term "customer entity" and "customer" are used interchangeably herein. Typically, mobile device customers 102 utilize the device management system 100 to manage mobile device services obtained from multiple service providers. A single customer 102 is illustrated in

FIG. 1 for simplicity; however, in another embodiment, the system 100 is capable of supporting multiple customers 102, and a single customer 102 may also comprise multiple organizations, for example, a subsidiary and parent or a group of affiliated companies with a common IT support and procurement organization.

[00031] In an embodiment, the device management system 100 adapts or customizes to conform to customer policies. As used herein, the term "customer policy" is a procedure, practice, strategy, business process, goal or business requirement of a customer 102. Customers 102 provide information regarding internal policies or procedures related to mobile devices, such as requirements for distribution of mobile devices, acceptable use of such devices, billing requirements, end user requirements, provisioning procedures, support procedures and requirements, and the like. The provided information is utilized or incorporated into the device management system 100 to ensure that mobile devices are managed in accordance with the needs and standards of the customer 102. In another embodiment, the device management system 100 supports multiple customers 102, where the policies obtained from customers 102 are used to adapt the device management system 100 for particular customers 102, resulting in each customer 102 receiving customized service provided by a unique combination of one or more service providers 104.

[00032] The device management system 100 obtains service provider data or information from one or more service providers 104. In one embodiment, the service provider data includes information regarding available service plans, devices, offers, discounts, and the like. Such information is utilized in conjunction with customer data to manage allocation, distribution, support and/or billing for mobile devices for customers 102 and other end users. In an embodiment, the service provider information includes information specific to a particular customer 102 that is predicated on specific sonic volumes. For example, a discounted rate negotiated by the customer 102. In addition, service provider information applicable to multiple customers 102 is reused, where the device management system 100 supports multiple customers 102. The service provider information also includes usage and billing data associated with the customer's 102 mobile devices and services. As used herein the terms "wireless devices" or "mobile devices," unless explicitly stated otherwise, includes both the mobile device hardware (*e.g.*, the mobile phone) and the service plan associated with that mobile device hardware. Such service provider information is utilized in administration, billing and optimization of mobile devices for customers 102.

[00033] In an embodiment, the device management system 100 is supported by a third party operator, which provides a single interface through which customers 102 manage mobile devices associated with multiple service providers. Customers 102 communicate with the device management system 100 using various modes of communication, such as voicemail, help desk, email, an Internet website, mobile device portal, or other user interface 202 (see Fig. 2). In one embodiment, the device management system 100 serves as a single point of contact for all mobile device issues, eliminating the necessity of determining the appropriate contact for various problems or issues.

[00034] The device management system can be implemented in a client-server model computing environment (*e.g.*, two-tier or multi-tier model). In particular, customers and service providers can correspond to clients, where the device management system corresponds to a server. Possible communications can be in the form of data packets transmitted among the clients and servers.

[00035] Referring now to FIG. 2, a more detailed block diagram of a device management system 100 is illustrated. The device management system 100 includes a user interface 202 with which customers 102 can access and direct mobile device management. In an embodiment, the user interface 202 is customized based upon the customer 102 and/or the particular end user or class of end user (*e.g.*, administrator, executive, sales personnel) utilizing the user interface 202. Using the login information or user credentials, the user interface 202 filters or hide options, ensuring that only those tools, features, and options available to a particular end user, as determined based upon customer data describing customer policies and practices and relevant service provider data.

[00036] In an embodiment, the user interface 202 is provided as a web application or set of applications accessible *via* a network, such as the Internet. The user interface 202 acts as a web portal that provides customers 102 and end users with a central location to access information related to multiple service providers 104 as well as multiple tools for use in procuring, billing, and managing mobile devices and can be customized to include customer branding. The content of the user interface 202 is adaptable based upon customer policies or practices. In an embodiment, the user interface 202 presents users with customer specific text, such as an Acceptable Use Policy (AUP) or response to frequently asked questions (FAQs). In addition to the text presented, the user interface 202, in some embodiments, is adapted to present or collect data from users as a function of customer policies and practices.

For example, a customer can define a policy describing a requirement that a particular category of end user, such as salesperson, always get a mobile device with wireless e-mail capabilities. In which case, when an end user who is a salesperson logs on to the system, the user interface 102 will only provide mobile device options with wireless e-mail capability. Although the user interface 202 is illustrated as a single component, the interface can be implemented as one or more distinct interfaces. For example, separate interfaces may be maintained for procurement and asset management.

[00037] In an embodiment, the device management system 100 includes a customer data store 204 that maintains information related to the procedures, policies and practices of one or more customers 102. This information allows the user interface 202 and other components to provide functionality specific to particular customers 102. As used herein, the term "data store" refers to any collection of data (*e.g.*, a database, collection of files or cache). In particular, the customer data store 204 maintains data such as particular device or service provider options available to the customer 102, and customer billing address and/or delivery addresses. Other service provider information can include, contact information, such as service provider representatives.

[00038] In certain embodiments, the customer data store 204 maintains organizational information as well as end user information for one or more customers 102. End user information is any data related to a customer's end users, including, but not limited to, end user position, password, access permissions, location, business unit, department, an exhaustive audit trail for the user account including moves, adds, changes, and deletes (MACDs). Organizational information includes information regarding business units, individual end users, positions, departments or any other information related to the structure or management of the organization. Such organizational information in some embodiments is utilized to provide customized functionality, ensuring that end users are provided with the appropriate access and options. For example, a salesperson ordering a new cell phone is limited to the specific devices and service plans for which sales personnel are authorized. At the same time, end users that are members of the accounting department are granted access *via* the user interface 202 to functions that provide for generation of reports, data and/or statistics related to cell phone usage throughout the customer 102 or a business unit or other business organizational component associated with the customer 102. The detailed customer information maintained in the customer data store 204 facilitates the device management

system 100 to tailor access, functionality and reports while optimizing mobile device use while minimizing costs within the constraints of the customer's IT policies and procedures.

[00039] The device management system 100 includes a service provider data store 206 that maintains service provider information associated with multiple service providers 104. Service provider information includes, among other details, details of specific service plans and mobile devices offered by the service providers 104. For example, service plans vary in function offered (*e.g.*, data access, voice, voicemail, text messaging, mobile data services, and email), fee policies (*e.g.*, fixed fee, limited usage, overage charges), coverage area, calling plans, calling restrictions, and the like. In addition, service provider information includes fees, rates, discounts and the like. In an embodiment, service provider information includes service plan, mobile device, billing or other options specific to one or more customers 102. For example, a customer 102 may negotiate with the service provider 104 for better rates based upon, for example, the number of end users, volume of calls made, or data transmitted or number of mobile devices.

[00040] An aggregation component 208 utilizes service provider data obtained from the service provider data store 206 combined with customer data obtained from the customer data store 204 to facilitate administration of mobile devices for customers 102. As used herein, the term "component" includes hardware, software, firmware or any combination thereof. For example, a component may be, but is not limited to being, a process running on a processor, or alternatively, the processor itself. Further, a component can be localized in a single computer or server, or distributed among two or more computers. The aggregation component 208 coordinates customer policies reflected in the customer data and service plan specifications obtained from multiple service providers 104 to assist the customer 102 in administering distribution, cost allocation, support and monitoring of mobile devices for end users associated with the customer 102. In another embodiment, the aggregation component 208 also utilizes end user data, such as end user position, location, business unit, department, an exhaustive audit trail for the user account including moves, adds, changes, and deletes (MACDs), as well as any other relevant end user information for administration of mobile devices. The aggregated service provider, customer data and end user data is useful for a number of functions that facilitate management of mobile devices, including, but not limited to, procurement of mobile devices, billing or invoicing for such devices and associated services, tracking mobile devices within a customer's organization and/or providing support for mobile devices.

[00041] In one embodiment, the device management system 100 includes a procurement component 210 that coordinates mobile device orders provisioning and distribution. Customers 102 access the procurement component 210 *via* the user interface 202 to place for orders for mobile devices and to track shipments of such devices. The procurement component 210 utilizes customer 102 and service provider 104 specific information to control device ordering, ensuring that mobile device selections are consistent with customer policies and service provider service plans. For example, the procurement component 210 utilizes customer data from the customer data store 204 to ensure that only those mobile devices or service plans approved by the customer 102 in accordance with customer's wireless policy are presented for selection by a user. The procurement component 210 utilizes provider service plan pricing that has been negotiated with the service providers 104.

[00042] In another embodiment, the procurement component 210 is customized based upon the specific individual or end user utilizing the procurement component 210. As described above, the procurement component 210 provides different mobile device options based in part upon the characteristics of the end user, such as end user data. For example, customer policies may provide for different mobile devices or service plans based upon characteristics of the end user, such as position within the organization, business unit, length of service and the like. In another embodiment, end users that act as mobile device system administrators for the customer 102 may have access to additional functions in the device management system 100, such as monitoring mobile device distribution across business units or approval of order requests or have their contact details forwarded to a service provider 104 as the designated contact. Other end users may be limited to narrower functions, such as ordering a device for their personnel use, or reviewing use and history unique to themselves.

[00043] In other embodiments, the procurement component 210 and user interface 202 ensure that a customer specific procurement process is followed in ordering mobile devices, as specified in customer data reflecting the customer's policies and procedures. For example, a customer 102 requires approval or authorization by specific individuals or departments before orders for mobile devices or services are placed with a service provider 104. Based upon customer data maintained in the customer data store 204, the procurement component 210 determines the appropriate individual, department or email address to contact for approval prior to placing the order with the appropriate service provider. In this manner, the device management system 100 is able to generate, follow, and administer the business

process necessary to comply with IT policy and procedures. In a further embodiment, the procurement process is specific to the particular end user ordering a mobile device. For example, the manager of the end user may be required to approve the order. Alternatively, certain end users (*e.g.*, executives) may not be required to obtain approval.

[00044] In another embodiment, the device management system 100 includes an asset component 212 that provides for monitoring and managing mobile device assets of customers 102. By accessing the asset component 212 *via* the user interface 202, selected end users obtain information regarding distribution and use of mobile devices for the customer 102. The asset component 212 is also used to generate reports indicating exceptional use characteristics, usage statistics, distribution characteristics and the like for both individual users and in the aggregate for groups of end users.

[00045] The asset component 212 accesses data maintained in an asset data store 214 to analyze, process and provide data to end users. In an embodiment, the asset data store 214 maintains information regarding the customer's mobile devices, including, but not limited to, information regarding employees that currently have access to specific assets, length of time employees have had assets, business unit and/or title of the employee holding the asset, billing and usage data, and the like. In another embodiment, package slips, invoices or any other forms associated with a mobile device are stored in the asset data store 214. In yet another embodiment, the asset data store includes data regarding mobile device connection cards and accessories (*e.g.*, ear buds, Bluetooth accessories and the like). The asset data store 214 maintains such data for mobile devices or assets obtained from multiple service providers 104. Collection of such data at a central location facilitates analysis and optimization of utility and use of mobile devices, while controlling or minimizing costs.

[00046] In a further embodiment, the device management system 100 includes a billing component 216 that directs billing and invoicing for mobile devices. Invoices and/or usage data from one or more service providers 104 is obtained by the device management system 100 and stored in the service provider data store 206. In one embodiment, the billing component 216 utilizes the aggregate information maintained in the service provider data store 206 to generate invoices. Invoice and/or usage data from multiple service providers 104 can be combined, separated based upon business unit, service type (*e.g.*, voice & data) or any other criteria useful to the customer 102. For example, employees may be billed for certain portions of their mobile device expenses (*e.g.*, personal phone calls, additional functions). In

an embodiment, customer policies define generation of separate invoices based upon aggregated information from multiple service providers. In addition, end users may utilize the billing component 216 to view, sort and analyze billing and usage patterns. In another embodiment, the billing component 216 is capable of automatically paying service provider invoices.

[00047] In still another embodiment, the device management system 100 includes a support component 218 that manages provision of support for mobile device users and/or administrators. Support may include responses to end user or administrator questions, reporting and correction of technical problems with a mobile device or service, and even replacement mobile devices. The support component 218 provides a central source to obtain support for mobile devices provided by multiple service providers 104. In particular, users can access the support component 218 *via* the user interface 202, which may include a web site or application, a help desk, or any other means of communication.

[00048] Turning now to FIG. 3, another embodiment of the device management system 100 is illustrated, depicting inputs 302 and outputs 304 of the device management system 100. The illustrated inputs 302 and outputs 304 are merely exemplary; additional inputs 302 and outputs 304 can be provided to the system 100 and/or generated by the system 100. Inputs 302 are communicated to the device management system 100 using a variety of methods, such as *via* a network (*e.g.*, the Internet), over a telephone system, text messaging or using any other suitable means of communication or transfer of information.

[00049] In an embodiment, inputs 302 to the device management system 100 include wireless orders or mobile device orders 306. In particular, end users associated with a customer 102 utilize the device management system 100 to order mobile devices, such as cell phones or service plans. In particular, end users utilize the user interface 202 to access the procurement component 210 and select from available options. In another embodiment, only options available to the particular end user are displayed. End users access the user interface 202 utilizing identifiers and/or passwords that identify and authorize user access. Based upon information retrieved from the customer data store 204 regarding the particular end user or user traits (*e.g.*, business unit, position in the company, etc.), the user is provided with a customized list of mobile device and service plan options. Available options are also determined based upon available service plans of various service providers 104. In another embodiment, the set of available options are reduced by filtering available options by the

customer policy for an end user with the characteristics of the end user accessing the user interface 202. In still another embodiment, the set of available options presented to the end user is ordered based upon criteria such as total ownership cost for the customer 102. In an embodiment, the mobile device options presented to an end user by the user interface 202 are based upon customer data, service provider and end user data.

[00050] In response to the mobile device order 306, the user receives a communication 308 approving or denying the mobile device order. As discussed above, in certain embodiments, the procurement component 210 utilizes customer practices and policies, including customer approval procedures required for procurement of a mobile device, to review, oversee, and approve the procurement of mobile devices. The procurement component 210 retrieves information regarding the particular customer 102 and/or end user from the customer data store 204. Based upon the retrieved customer policies and authorization or denial from an appropriate party, the approval or denial communication 308 is communicated to the end user. In one embodiment, the denial communication is accompanied by a request for additional information and includes a link or form for the end user to submit or input such additional information. For example, approval can be delivered via email, voicemail, or any other suitable means of communication. If the order is approved, the end user may be provided with a confirmation notice 310 once the order is placed with the appropriate service provider 104.

[00051] In another embodiment, the device management system 100 receives a bulk mobile asset load 312 as input 302. During initial setup or customization of the device management system 100 for a customer 102, mobile device records are processed in bulk or batches and added to the asset data store 214. The bulk mobile asset load 312 data may require reformatting or merely a customized mapping or input filter to sort the data to the appropriate fields with the asset data store 214 and can be provided as an electronic file or set of files. The information is parsed and transformed into the device management systems 100 standard format by the asset component 212. The reformatted data is then stored within the asset data store 214. As additional mobile devices are added by the procurement component 210, the data related to the new mobile devices is stored in the asset data store 214. Contemporaneous to loading of mobile device information, customer policies, procedures, organizational information and other data related to the customer 102 is uploaded or entered into the customer data store 204.

[00052] In other embodiments, end users obtain or receive mobile asset management reports 314 that provide customers 102, users and administrators with data regarding distribution and usage of mobile devices by the customer 102 and the customer's end users. The information can be presented in a variety of formats to assist customer 102 in monitoring and managing mobile devices. In an embodiment, reports 314 describing asset distribution and usage are generated periodically or dynamically at the request of an administrator or end user. The reports 314 can be used to optimize utility of mobile device distribution and can be distributed through email, traditional hard copy or using any other suitable method of communication.

[00053] In still another embodiment, customer administrators obtain or receive asset exception reports 316. These exception reports 316 describe instances of usage that may be particularly useful in optimizing mobile device use and minimizing mobile device fees. For example, exception reports 316 can list mobile devices or end users incurring the largest roaming charges or exceeding minute limitations. In yet another embodiment, the exception reports 316 provide details of usage of the mobile device by an end user that is potentially indicative of a violation of the customer 102 IT policy or Acceptable User Policy. In an embodiment, reports are customized based upon customer policies specified in the customer data store 204. Such reports can be automatically generated and sent to a predetermined customer email address and/or generated upon request. Exception reports 316 are described in further detail below.

[00054] The device management system 100 also receives reports of support incidents 318. Support incidents include updates to mobile devices, such as moves, adds, changes, deletions (MACDs), as well as, failure, malfunction, theft or loss of a mobile device. The user interface 202 can include a call center or electronic voice phone system that receives communications reporting support incidents. Reports of support incidents are utilized by the support component 218 to provide assistance to users. In an embodiment, replacement mobile devices are supplied to users experiencing mobile device difficulties. In addition, reports of support incidents are tracked, analyzed and used generate support reports 320. In particular, data related to failure of particular devices is maintained in the asset data store 214. Information regarding mobile device failures and end user problems, as well as responses to such problems, is output in support tracking reports 320.

[00055] The device management system 100 receives usage records or billing data and call detail records 322. In particular, usage data from multiple service providers 104 is received and entered into the system 100. This information is maintained in the service provider data store 206 and utilized by the billing component 216 to allocate, monitor, control, or direct billing. In one embodiment, the billing component 216 generates invoices as a function of the provided billing data and call detail records. The invoices can be customized based upon individual customer practices and procedures. For example, costs may be grouped by business unit, rather than by service provider. Additionally, distinct services from a single carrier can be invoiced separately or multiple carrier invoices can be consolidated into one invoice.

[00056] The billing component 216 generates one or more reports reflecting billing and usage information. For example, a cost allocation report 324, detailing mobile device expenses, allocates costs by business unit, service provider 104, employee or end user classification or characteristic or any other useful category. In addition, the billing component 216 can generate a call usage detail report 326 providing customers 102 with detailed information regarding use of mobile devices. Such reports can be formatted or organized in any manner useful for the customer 102 and may be customized based upon customer policies. In addition, the billing component 216 generates custom invoices 328 based upon customer policies.

[00057] Referring to now FIG. 4, a detailed block diagram of an embodiment of the procurement component 210 is illustrated. The procurement component 210 provides end users with a tool for obtaining mobile devices and services from one or more service providers 104. The procurement component 210 coordinates placement mobile device orders, processing and authorizing of such orders, as well as monitoring shipment and provisioning of mobile devices. In particular, end users interact with the procurement component *via* the customizable procurement user interface 400. As described above, the procurement user interface 400 can be implemented as a stand-alone user interface, or as a part of a general interface 202 to the device management system 100.

[00058] In an embodiment, the procurement user interface 400 is available *via* a network, such as the Internet. In another embodiment, a graphical user interface (GUI) is provided, allowing users to select from available mobile device and service options. Options are displayed based upon customer policies and service provider data, such as available

service plans. In particular, the service plans selected by the customer from one or more service providers affect available options presented to end users. In addition, options presented to individual users vary based upon the user characteristics or traits, including, but not limited to, user business unit, user position within the company or any other relevant characteristic. In an embodiment, the procurement user interface 400 utilizes customer-specific information or policies expressed in the asset data store 214 to provide customized options.

[00059] The procurement component 210 includes an order component 402 that manages placement orders of mobile devices. In particular, the procurement component 210 receives information from the procurement user interface 400 regarding selected options and generates one or more order to be communicated to service providers. When configured, the order component 402 can automatically submit secure email orders or requests to the appropriate service provider or service providers.

[00060] In another embodiment, the procurement component 210 includes an authorization component 404 that verifies or obtains authorization for an order generated by an end user. Many customers require authorization by specific employees or departments prior to purchase of equipment. The authorization component 404 utilizes the specific authorization procedures of the particular customer 102 with which the user is associated to authorize the purchase order. The authorization process is expressed as a customer policy described in the customer data store. In an exemplary approval process, the authorization component 404 notifies a particular individual or department (*e.g.*, an information technology (IT) department) of the customer 102 with authority to approve orders. In another embodiment, the individual with authority to approve orders varies based upon the particular user placing the order. For example, the customer 102 may require approval of the manager of the user. End user information and customer hierarchy or organization information maintained in the customer data store are used to identify the individual with authority to approve the order. In one embodiment, the authorization component 404 sends an email or other electronic notice to the appropriate authority. In another embodiment, the authorization component 404 generates the appropriate customer forms and sends an electronic or hard copy of the forms to the relevant authorities. Approval or denial can be communicated *via* a response to an email request, *via* the procurement user interface 400, or using any other mode of communication.

[00061] Once approved, the order is communicated to the appropriate service provider. In an embodiment, the procurement component 210 also includes a tracking component 406 that monitors filling and delivery of the ordered equipment. The tracking component 406 obtains status information regarding the progress and/or estimated date and time of delivery of the mobile device. In addition, the tracking component 406 can track the shipping of the mobile device to the particular user. The tracking component 406 obtains shipping information from the service provider 104 and monitors the progress of the shipment. In an embodiment, the tracking component 406 can notify the user of progress (*e.g.*, time of shipping, estimated delivery date, progress of package) *via* email, voicemail, text message or any other form of communication. In addition, the user can obtain status information from the tracking component 406 through the procurement user interface 400. Once the mobile device and the order completed, information regarding the asset is stored in the asset data store 214 as a part of the inventory of the customer 102.

[00062] With reference to FIGs. 5, 6, 8, 9, 11, 12, 14-17, flowcharts depicting methodologies associated with management of mobile devices are illustrated. For simplicity, the flowcharts are depicted as a series of steps or acts. However, the methodologies are not limited by the number or order of steps depicted in the flowchart and described herein. For example, not all steps may be necessary; the steps may be reordered, or performed concurrently.

[00063] Turning now to Fig. 5, an exemplary methodology for processing a user order is illustrated. At reference number 502, an order is generated by the order component 402 based upon input provided by users through a user interface 202. In an embodiment, orders are generated using customized user interface 202 that ensures that orders comply with customer practices and policies. An order includes data regarding the end user creating the order, the mobile device, including physical device and service plan, requested and the service provider 104 from which the mobile device is to be purchased or supported. In addition, the order can include information such as delivery address, business unit responsible for billing purposes and the like.

[00064] At reference number 504, authorization for the order is requested by the authorization component 404. In an embodiment, the individual order or authorization procedures of the customer 102 determine the authorization process. In particular, customer authorization policies are described in the customer data store and used to control order

processing. For example, an email can be transmitted to the appropriate party (*e.g.*, manager of the requesting user, IT department, and the like) requesting authorization of the order. In an embodiment, the authorization component 404 utilizes the standard requisition form of the company to request authorization of the order. At 506 a determination is made as to whether the order is authorized. If no, at reference number 508, the user who generated the order is notified that the order has not been authorized and will not be processed. The process then terminates.

[00065] If the order is authorized, the service provider104 is notified and provided with the order information at reference number 508. In addition, the end user may be notified of approval and placement of the order. Once the order is placed, the tracking component 406 obtains tracking and/or shipping information from the service provider 104 at reference number 510. Shipping information can include an estimated time to shipment of the mobile device or devices to fill the order, a tracking number used by the delivery service, an estimated date of delivery, and any other information related to delivery of the mobile device(s). At reference number 512, the tracking component 406 tracks or monitors delivery of the mobile device(s). For example, the tracking component 406 retrieves tracking information from the delivery service, provides users with updates regarding status of the order (*e g.*, email specifying date shipped and status in transit) and the like. The order component 402 can update asset data store 214 to reflect the addition of new mobile devices or changes to existing mobile device accounts at reference number 514.

[00066] Turning now to FIG. 6, an exemplary methodology for adding or updating mobile device information in the asset data store 214 in response to completion of an order is illustrated. After an order is placed, and the mobile device delivered to the end user, the asset data store 214 is updated to reflect the new information. The mobile device may be provided to an end user that does not have an existing, associated wireless number. For example, a new employee may be provided with a mobile device assigned a new wireless number. Alternatively, an existing end user may replace an existing mobile device associated with a particular wireless number, with a new mobile device. In which case, the new device is to be associated with the pre-existing wireless number in the asset data store 214. In addition, wireless numbers that have been unused for a period of time, becoming historical records rather than active accounts, may be reissued with the new mobile device.

[00067] At reference number 602, the status of the order is updated upon delivery of the mobile device to the end user and new mobile device information is to be added or updated in the asset data store 214. At reference number 604, the wireless number assigned to the delivered device is compared to mobile device data maintained in the asset data store 214. In an embodiment, the wireless number itself is used as an identifier for a mobile device. If the mobile device is a replacement for an existing device, the wireless number will already exist within the asset data store 214.

[00068] At reference number 606, a determination is made as to whether the wireless number already exists within the asset data store 214. If no, the mobile device is added as a new record to the asset data store 214 at reference number 608, and the process ends with addition of the new mobile device record. However, if the wireless number already exists within the asset data store 214, a determination is made as to whether the record associated with the wireless number is a historical record at reference number 610. Wireless numbers and related data associated with a mobile device that is not in active use are maintained by the asset data store 214 as historical records, preserved for use in analysis, comparison and the like. If the status of the wireless number record in the asset data store 214 is that of a historical record, status is updated to active and the new mobile device is added to the asset data store 214 at reference number 608.

[00069] If the wireless number currently exists in the asset data store 214 and is not marked a historical record, then the wireless number is in active use. At reference number 612, a determination is made as to whether the customer 102 indicated in the order matches the customer 102 associated with the wireless number record in the asset data store 214. If no, then the wireless number has been reallocated or transferred from the customer 102 referenced in the asset data store 214 to the customer 102 placing the order. Accordingly, the record in the asset data store 214 is marked as a historical record at reference number 614, since the wireless number is no longer active for that customer. The mobile device is added to the asset data store 214 as a new wireless number record for the customer 102 indicated on the order at reference number 608.

[00070] If the customer 102 indicated on the order matches the customer 102 associated with the wireless number in the asset data store 214, then at reference number 616, a determination is made as to whether the carrier or service provider 104 referenced in the order matches the service provider 104 associated with the wireless number in the asset data

store 214. If the service provider 104 associated with the order does not match the service provider 104 referenced in the asset data store 214, the wireless number has been transferred from one service provider to another. At reference number 614, the wireless number record in the asset data store 214 is marked as a historical record, and the mobile device in the asset data store 214 is added as a new wireless number record associated with a new service provider 104 at reference number 608.

[00071] If the service provider 104 and customer 102 match the information maintained in the asset data store 214 associated with the particular wireless number, then at reference number 618, the wireless number is updated for the new mobile device utilizing information from the order. In this scenario, the physical device has been updated, but there is no need to create a new record since the service provider 104 remains the same.

[00072] FIG. 7 is a detailed block diagram of an exemplary embodiment of the asset component 212. Users interact with the asset component 212 primarily through an asset management user interface 700. As described above, the asset management user interface 700 can be implemented as a stand-alone user interface, or as a part of a general interface 202 to the device management system 100.The asset component 212 provides detailed information regarding the distribution and use of mobile devices through the organization, which is presented *via* the customized asset management user interface 700. In an embodiment, users are identified and granted access to mobile device information in accordance with the customer policies, as specified in the customer data store 204. Access may be limited based upon business unit, or function of the end user within the customer (*e.g.*, administrator or salesperson) For example, upper level managers are likely to be granted significantly wider access than end users in sales departments.

[00073] In an embodiment, the asset component 212 includes a management component 702 that provides users with the ability to monitor and manage mobile devices associated with the customer102. The management component 702 may be accessed *via* the asset management user interface 700 and used to retrieve information regarding one or more mobile devices and/or mobile device usage from the asset data store 214. In another embodiment, the management component 702 has one or more pre-defined queries or data retrieval functions that provide relevant data to users. Data retrieval is limited to assets specific to the customer 102 requesting the data, and may be customized based upon the user requesting the data, business units, organizational hierarchy or other criteria.

[00074] The management component 702 modifies records maintained in the asset data store 214, the customer data store 204 and service provider data store 206. In an embodiment, administrators utilize the management component 702, accessed *via* the asset management user interface 700, to update or correct data in the asset data store 214, customer data store 204 or service provider data store 206. In particular, end user information can change as end users are added, transferred or leave the customer. Similarly, new mobile devices are purchased or leased and existing mobile devices are transferred to other end users or become worn out and are retired. In addition, service plans and customer needs vary over time. Accordingly, end user, mobile device and service provider information maintained in the asset data store, customer data store 214 and service provider data store 206 are updated to reflect these changes.

[00075] In another embodiment, updates or modifications by an end user require approval, similar to the approval process required to procure a mobile device. For example, a disconnect of a mobile device, addition or removal of services (*e.g.*, text messaging or international dialing) or a change in user information (*e.g.*, change in position, employment status, business unit or the like) may require approval of the end user's manager. In such cases, customer policies regarding authorization of modifications to end user or mobile device data are retrieved from the customer data store 204 and the appropriate individual or entity is contacted for approval prior to modification of the data within the asset data store 214, customer data store 204 and/or service provider data store 206.

[00076] In other embodiments, the management component 702 identifies mobile devices at the end of their lifecycles as candidates for retirement. A report is generated listing candidate mobile devices that have been in service greater than specified period of time. An administrator can select from the list of mobile devices for upgrade or replacement. Upon approval by an administrator, end users are notified of a replacement mobile device, which may be obtained *via* the procurement component 210, and are required to return the retired mobile devices. The management component 702 can track the return and recycling or destruction of retired devices.

[00077] The asset component 212 also includes a reporting component 704 that generates one or more reports regarding customer mobile devices. The reports may be based upon usage of devices, billing for mobile devices or any other statistics. The report data may be collected and filtered for specific business units, individuals, or particular functions or

service plans. In an embodiment, the reporting component 704 periodically generates a set of reports, including specific reports directed to executive level end users and mobile device administrators. In another embodiment, the reporting component 704 generates customized reports based upon end user elections input *via* the asset management user interface 700.

[00078] The reporting component 704 provides customers 102 or end users with exception reports 316. Exception reports 316 identify unnecessary or unusual usages, resulting addition or increased service provider charges. In an embodiment, exception reports 316 detail directory assistance charges, equipment charges (*e.g.*, support, replacement or repair fees), and roaming charges. In another embodiments, the exception report 316 lists top users of mobile devices, end users who did not utilize their mobile device at all during the reporting period, and end users that accumulated data charges.

[00079] The asset component 212 includes an optimization component 706 that analyzes data associated with a particular customer 102 and generates recommendations to optimize mobile devices based upon customer policies or strategies. Common strategies include minimization of cost to the customer 102 while maintaining necessary functionality. In an embodiment, the optimization component 706 utilizes the statistics collected by the reporting component 704 to identify likely optimization opportunities.

[00080] In other embodiments, the optimization component 706 identifies opportunities for reducing costs and provides suggestions or recommendations for optimizing mobile device distribution for the customer 102. The optimization component 706 details the particular steps to minimize cost while maintaining functionality. For example, the optimization component 706 can identify users with the highest overages (*e.g.*, minutes in excess of the amount allotted by the service plan) and recommend switching such users to a service plan without a maximum number of minutes. Similarly, users who consistently utilize only a fraction of the available minutes can be identified for transfer to a service plan with reduced minutes. The optimization component 706 can periodically analyze customer statistics. Alternatively, users can request optimization recommendations at any time, *via* the asset management user interface 700.

[00081] The optimization component 706 is customizable and may be trainable. In an embodiment, frequency of optimization as well as particular statistics for analysis and other features are customizable for the particular customer. In addition, the suggestions or possible optimizations are based upon the particular characteristics of the customer 102. For example,

optimizations are based upon standard market offers or deals negotiated by the customer 102 with particular service providers and other customer policies.

[00082] In an embodiment, the optimization component 706 includes or consists of artificial intelligence or knowledge or rule-based components, methodologies or mechanisms. For example, the optimization component uses vector machines, neural networks, expert systems, Bayesian belief networks, fuzzy logic, data fusion engines, classifiers or the like. Accordingly, the optimization component is adaptive over time and may become more efficient in identifying opportunities and generating recommendations.

[00083] Referring now to FIG. 8, an exemplary methodology for optimizing mobile devices for a customer is illustrated. At reference number 802, one or more exception reports 316 are generated. Such reports identify mobile devices operating outside normal bounds, or mobile devices operating at the extremes. For example, exception reports identify such as the most and least used mobile devices and functions. In an embodiment, exception reports 316 are based upon the most recent billing and usage data. In a further embodiment, historic information regarding billing and usage is obtained, averaged and used to identify exceptions. In yet another embodiment, a weighted average of the most recent billing and usage data as well as historical billing and usage data is utilized.

[00084] At reference number 804, the exception reports 316 are exported to either the customer 102, or the customer data store 204. These exception reports 316 are maintained in summary files at reference number 806. At reference number 808, the exception reports 316 and summaries are analyzed to determine defects that indicate possible opportunities for optimization. In an embodiment, analysis includes comparison with predetermined standards of usage, utilization or other statistics. Alternatively, the determination is based upon comparison with historical data, average usage and the like.

[00085] Based upon the analysis of charges and identification of defects, a list of defects and associated recommendations for resolving such defects is generated at reference number 810. Recommendations can be customized for the particular customer 102. In particular, the recommendations are based upon the various negotiated plans or options with various service providers. In addition, in certain embodiments, such recommendations are a function of the particular practices and policies of the customer 102, such as options available within business units, and the like. A summary of exceptions and associated

recommendations is produced at reference number 812. The resulting exception and recommendation report is communicated to the customer 102 at reference number 814.

[00086] The customer approves or ignores the various recommendations. At reference number 816, a determination is made as to whether the customer 102 approves of each of the one or more recommendations. For each recommendation not approved, the suggestion is documented for future reference at reference number 818, but not implemented. For each recommendation approved, the approved change in service is submitted to the appropriate service provider 104 at reference number 820. At reference number 822, the changes to the service plans are confirmed. The optimization process can be repeated periodically, (*e.g.*, on a monthly or quarterly basis) or dynamically triggered by an end user.

[00087] Referring now to FIG. 9, a flowchart depicting an exemplary methodology for optimizing mobile device management by reducing costs is illustrated. At reference number 902, billing and/or usage data is obtained from one or more carriers or service providers. The received data is reformatted and combined at reference number 904. The combined data is analyzed to identify potential optimization of various recurring charges.

[00088] Recurring charges are predictable, periodic charges, such as monthly basic cell phone charges. Optimization recommendations to minimize recurring charges based upon actual usage of the services for which monthly charges are accrued are generated. In particular at reference number 906, the optimization component 706 analyzes the combined data to optimize use of minutes for voice communications. For example, a service provider 104 may provide several service plans with different amounts of prepaid minutes. Recommendations for switching between service plans are generated based upon actual use of minutes during the previous period(s). In addition, the optimization component 706 generates recommendations for switching mobile devices between different service providers 104 to minimize overall cost for the customer.

[00089] In another embodiment, recurring charges include base fees for text messages or paging service. At reference number 908, the optimization component 706 optimizes text messaging recurring charges. Service providers 104 may provide different service plans that include various numbers of free text messages before applying additional overage charges for text messaging. Recommendations for switching between service plans are generated based upon if the end-user is utilizing text messaging or if they have incurred overage charges during the previous period. In an embodiment, an operator or administrator utilizes the

optimization component 706 to review exception reports 316 to identify opportunities for reducing costs and/or optimizing use of text messaging. In an additional embodiment, the optimization component 706 generates recommendations for switching mobile devices to different text messaging plans to minimize overall cost for the customer.

[00090] At reference number 910, the optimization component 706 generates recommendations to reduce data usage costs. Many mobile devices provide access to data. For example, many smart phones allow access to email accounts and/or the Internet. Typically, an additional fee is charged for such services. The optimization component 706 evaluates actual usage of the data services to identify opportunities to minimize costs while maintaining useful services. These recurring charges, as well as any other additional recurring charges, are summarized by the optimization component 706 in a summary of recurring cost savings at reference number 912.

[00091] In certain embodiments, the optimization component 706 evaluates variable costs and identifies opportunities to minimize costs. For example, at reference number 914, the optimization component 706 identifies instances where users incurred roaming charges. Many service providers 104 charge an extra fee, referred to as a roaming charge, when a user places or receives a call from outside the network of the service provider. The optimization component 706 identifies instances and trends of roaming charges and evaluates the frequency and amount of such charges. The optimization component 706 then generates recommendations based upon the roaming costs. For example, the recommendation may suggest switching the mobile device to a new service plan that would reduce or eliminate roaming fees.

[00092] The optimization component 706 also identifies directory assistance costs at reference number 916. Directory assistance fees are incurred when users call the service provider 104 or an operator and request a telephone listing. Recommendations to avoid such costs can include training employees who make repeated calls for directory assistance to avoid such calls.

[00093] In another embodiment, the optimization component 706 analyzes the billing and usage data to identify users who did not utilize mobile devices or various mobile device functions in the preceding billing period at reference number 918. Such users may have no need for the device at all, in which case the mobile device can be returned or reassigned. The optimization component 706 may generate a recommendation that the users need for the

mobile device be reevaluated. A summary of the variable costs is produced at reference number 920.

[00094] The optimization component 706 merges the recurring and variable cost summaries and recommendations at reference number 922. The generated summary includes identified, exceptional costs as well as recommendations to minimize such costs. The summary can be a high-level or detailed report depending upon the requirements of the particular customer 102. At reference number 924, the summary is presented to the customer 102. For example, the report may be presented in a live consultation, and/or automatically generated and transmitted *via* email on a regularly basis. Alternatively, a printout may be provided on a periodic basis, such as monthly or quarterly. In another embodiment, an administrator associated with the customer logs into the mobile device management system 100 *via* the Internet and triggers generation of the report. In an embodiment, the report is presented as a static document. Alternatively, the report can be provided using the graphic user interface 202 and allowing users to elect to view detailed, underlying data.

[00095] Based upon the response(s) of the customer, a determination is made as to whether to process one or more of the recommendations at reference number 926. The recommendations which are declined are recorded at reference number 928. These recorded recommendations may be used in future analysis of recommendations. In particular, recommendations that are consistently ignored by customer are devalued, with the result that such recommendations are less likely to be generated in the future.

[00096] At reference number 930, a service change request is submitted to one or more service providers 104 based upon the approved recommendation(s). In an embodiment, the service change request(s) are submitted by an operator or administrator. Alternatively, the service change requests are automatically submitted by the optimization component 706. After submission of the requests, implementation of the requested changes by the service provider 104 is confirmed at reference number 932. This confirmation is provided to the customer at reference number 934. The process then terminates, but may be repeated periodically. For example, optimization may occur on a monthly or quarterly basis.

[00097] FIG. 10 is a block diagram of an exemplary support component 218. The support component 218 manages assistance for users experiencing problems with a mobile device and provides a central location for assistance regardless of the particular service provider 104 that issued or supports the mobile device. In addition, the support component

218 tracks support incidents, maintaining incident reports in a support data store 1002, and assisting administrators in ensuring adequate support and reducing mobile device problems. In an embodiment, the support data store 1002 is associated with the asset data store 214, providing an exhaustive audit trail detailing the entire support history of a mobile device. In general, users and administrators interact with the support component 218 *via* the user interface 202. In addition, the support component 218 may be associated with a help desk that provides phone support for users. Either an automated telephone system or help desk personnel may interact with the support component 218, typically *via* the user interface 202, to provide the users with the assistance required.

[00098] The support component 218 includes a support response component 1004 that utilizes data obtained from the asset data store 214 and/or service provider data store 206 to assist users. Support is provided in accordance with customer policy described in the customer data store 204. Support service can include responding to end user questions, troubleshooting problems and/or temporary suspension of services if a mobile device is misplaced. Service may be resumed if the device is located, or the mobile device may be replaced if permanently lost or stolen. In an embodiment, a replacement mobile device is provided to the user when the user's device is damaged, lost or broken (*e.g.*, dropped, immersed in water, and the like). The support response component obtains information regarding the details of the mobile device from the asset data store 214 to ensure that the replacement mobile device has identical or substantially similar functionality. In certain embodiments, the support response component 1004 directs the delivery of the replacement device to the user. Delivery of a replacement may be provided by the operator of the device management system 100. For example, the device management system operator may provide a replacement immediately from an inventory maintained by the operator to ensure rapid response to problems. Alternatively, the support response component 1004 directs the service provider 104 to ship a replacement mobile device to an end user.

[00099] In another embodiment, the support component 218 includes a warranty component 1006 that facilitates management of repair and replacement policies of various service providers. In an embodiment, warranty information is associated with the mobile device record in the asset data store 214. In an embodiment, upon request from a user for a replacement, an administrator or operator determines if replacement is truly necessary (*e.g.*, troubleshoots the mobile device) and if necessary, utilizes the warranty component 1006 to generate an order and/or submit the order for the replacement to the appropriate service

provider 104. In another embodiment, the warranty component 1006 automatically generates and/or submits forms or paperwork necessary to comply with the various service plans of individual service providers 104. In yet another embodiment, the forms are submitted to the customer 102 for approval, before being submitted to the service provider. Administrators can monitor both receipt of the replacement mobile device, and return of the broken mobile device. In certain embodiments, the warranty component 1006 generates a reminder to ensure that the service provider applies the warranty device replacement credit to the end users invoice.

[000100] The support component 218 also includes a support reporting component 1008 that provides administrators with the ability to review requests for support and responses by the device management system operator and/or individual service providers 104. Such support information is important in evaluating service providers 104 and ensuring necessary support is provided. In addition, the support component 218 analyzes the support records to identify trends, such as mobile device models prone to failure or individuals prone to damaging or losing mobile devices. Support records maintained in the support data store 1002 provide an audit trail for a mobile device's support history as well as supporting service level agreement (SLA) performance metrics.

[000101] Turning now to FIG. 11, an exemplary methodology for responding to a request for support is illustrated. At reference number 1102 a request for support is received by the device management system 100. The request can be received *via* the user interface 202, an automated phone system, email, an operator at a help desk or using any other suitable means for communication. A response confirming receipt of the request is communicated to the user at reference number 1104. The response can be transmitted by text message, email, voicemail or any other suitable communication method. In an embodiment, the response includes an estimated time to delivery of a replacement mobile device. In a further embodiment, the device management system operator maintains a stock of mobile devices and ships the devices upon receipt of a support request, enabling rapid response to failure of a mobile device (*e.g.*, delivery of replacement within twenty-four (24) hours of support request).

[000102] In another embodiment, at reference number 1106, the support response component 1004 contacts the appropriate service provider 104 to prompt the service provider 104 to respond. In addition, various forms can be submitted to the service provider 104 by

the warranty component 1006 based upon warranty or service plan negotiated with the service provider 104. Information regarding the specific requirements for support from a service provider 104 is retrieved from the service provider data store 206.

[000103] At reference number 1108, the shipment of a replacement mobile device is tracked by the support reporting component 1008. In an embodiment, the support reporting component 1008 provides status updates (*e.g.*, estimated time to delivery or current location of shipment) to the user awaiting the arrival of the replacement mobile device. Status updates can be provided by email, text messages or any other means of communication. In another embodiment, the user can access the support reporting component 1008 *via* the user interface 202 to obtain status information.

[000104] The delivery of the replacement is confirmed at reference number 1110. All or any portion of the support request and response process is maintained in the support data store 1002 at reference number 1112. Such information is useful in analyzing adequacy of support as well as possible problems in mobile devices or individual usage. At reference number 1114, the support response component 1004 updates the asset data store 214 based upon replacement of the mobile device.

[000105] Referring now to FIG. 12, a methodology for monitoring and optimizing provision of support for mobile devices is illustrated. At reference number 1202, support information is reviewed by users or customer administrators. In an embodiment, an administrator can periodically review support records to ensure that effective support is being provided. Alternatively, a report of each support record can be transmitted to an administrator or customer representative at the time of the incident. In another embodiment, an administrator can view support records using the support reporting component 1008 *via* the user interface 202.

[000106] At reference 1204, incidents where support was inadequate or untimely are flagged for attention. Such support records can be emailed to representatives at the customer 102 and or the device management system operator for redress. In addition, statistics regarding support incidents, response and the like can be provided for analysis. At reference number 1206, support records are analyzed and device specific trends are evaluated. In particular, the type of mobile device with the highest failure rate is identified. If the failure rate is out of the normal expected range, a recommendation may be generated to avoid the mobile device. At reference number 1208, user trends are identified. For example, certain

users are more likely to damage, lose or destroy mobile devices. Such users may be provided with more rugged devices. Alternatively, such users may be provided with less expensive devices.

[000107] Turning now to FIG. 13, a detailed block diagram of an exemplary billing component 216 is illustrated. The billing component 216 manages billing and usage data received from one or more service providers 104. In one embodiment, the billing component 216 includes an allocation component 1302 that handles cost allocation and invoices, including usage data, received from one or more service providers 104. Data may be received in a variety of formats in electronic files, *via* an electronic data interchange (EDI) feed, or in any other format utilized by a service provider. Data received from each service provider 104 is parsed, analyzed and reformatted into a standard format utilized by the device management system 100. Data standardization allows for combination and analysis of data from multiple service providers. In addition, the use of a standardized format facilitates the storage, maintenance and analysis of billing and usage data.

[000108] In an embodiment, the allocation component 1302 allocates costs from service provider invoices as a function of customer policies. Frequently, customers 102 purchase services (*e.g.* minutes of voice communications) at the macro or account level to receive the best rates from the service provider. The allocation component 1302 is able to report actual usage as a function of business unit or individual user, facilitating allocation of costs internally for the customer 102. In an embodiment, the allocation component 1302 takes into account all impacted values, such as monthly discounts, taxes and the like. Accordingly, the customer 102 is able to take advantage of cost savings by purchasing services at the organization-wide level, while allocating expenses at the business unit level.

[000109] In a further embodiment, the billing component 216 includes a payment processing component 1304 that handles payment of the service provider invoices. For example, the payment processing component 1304 charges customer 102 or even end user credit cards to facilitate payment of service providers. The payment processing component 1304 may utilize customer or end user credit card information maintained in the customer data store 204 to pay service provider invoices. In another embodiment, the payment processing component 1304 distributes paper invoices.

[000110] The billing component 216 includes a reconciliation component 1306 that correlates the standardized data received from the various service providers 104 with data

maintained in the asset data store 214 and even data from the customer data store 204. The reconciliation component 1306 reconciles the data sets and identifies inconsistencies. In an embodiment, corrective action is taken based upon the identified inconsistencies. Corrective actions include, but are not limited to, removal of inactive mobile devices from the asset data store 214, correction of name mismatches and addition of mobile devices missing from the asset data store 214. In other embodiments, inconsistencies are flagged for further review and can lead to dispute of certain service provider charges. In this manner, the invoice information from service providers 104 is verified prior to payment.

[000111] The reconciliation component 1302 is also capable of generating bills based upon the data received from various service providers. In an embodiment, costs are separated based upon functionality. In particular, users may be billed for certain functions (*e.g.*, voice communication charges), while the customer 102 pays for functions required by the customer 102 (*e.g.*, email access). Separate invoices can be generated for individual users, customer business units or third parties.

[000112] In another embodiment, costs are allocated to third parties, such as customer clients. This feature is particularly useful where the customer 102 is able to bill a client for phone charges incurred in the process of providing services to the client, such services that require long distance or overseas phone calls. The allocation component 1302 provides the capability to separate out charges based upon mobile number or cost center.

[000113] It is understood that various components and subcomponents illustrated in the block diagram figures can be rearranged or reorganized, by one of ordinary skill in the art. For example, the reconciliation component 1306 and allocation component 1302 are shown in FIG. 13 as subcomponents of the billing component 216. However, in an alternate embodiment, the reconciliation component 1306 and allocation component 1302 are separate and distinct components, rather than subcomponents of a billing component 216.

[000114] FIG. 14 is a flowchart depicting an exemplary method for transforming service provider information. At reference number 1402, billing and/or usage data is obtained from one or more service providers. The service providers 104 can utilize various methodologies to provide the data, including email, an EDI feed, file transfer protocol (FTP) or any communication means. Once received, the billing and usage data is parsed as a function of the service provider specific formatting to extract billing and usage data at reference number 1404. In particular, the invoice component 1302 obtains format information from the service

provider data store 206 and parses the received data in accordance with the format information to extract the desired information.

[000115] At reference number 1406, the invoice component 1302 transforms the extracted data into the standardized format of the device management system 100. Transformation can include translation of specific codes utilized by the service provider. This standardized format allows data from separate service providers 104 to be evaluated, compared, and combined. Standardization also allows for storage of the data in a central data store. At reference number 1408, the transformed data is loaded into the service provider data store 206. Maintenance of historic usage and billing information in a standardized format allows for analysis of billing and usage data over time, which may facilitate the identification of trends in usage.

[000116] Turning now to FIG. 15, an exemplary methodology for processing service provider invoices is illustrated. At reference number 1502, service provider information is obtained. The information may be the monthly invoices commonly received from service providers. The data may include detailed billing and usage information. The received data is reformatted as standardized data at reference number 1504. In an embodiment, reformatting includes extraction of data from the service provider format, transformation into the standardized format and loading into the service provider data store 206.

[000117] The standardized data is reconciled with data maintained in the asset data store 214 at reference number 1506. In one embodiment, the wireless numbers are verified and the services or functions are compared to the service for which the user has subscribed. In another embodiment, the charges are compared to the negotiated rates and service plans. Suspicious, inconsistent or invalid charges are flagged for further attention.

[000118] At reference number 1508, the invoice component 1302 generates invoices based upon the received data. The invoices are customized for the particular needs of the mobile device customer 102. In one embodiment, charges are divided and billed based upon business unit. In another embodiment, charges are divided based upon function or service provided (*e.g.*, data access, text messaging and the like), or upon usage. Invoices can be generated for the customer 102, one or more end users or third parties. For example, particular phone numbers are identified as personal use. Charges to such personal numbers are invoiced to the end user rather than the customer 102. In addition, phone numbers for

particular third parties, such as clients, can be identified. Charges associated with such third parties may be itemized and the third parties may be invoiced for the particular expenses.

[000119] The payment processing component 1304 pays the service providers 104 at reference number 1510. In an embodiment, the device management system 100 may be granted the right to pay undisputed service provider charges. In particular, credit card information for the customer 102 is provided to the device management system 100 and utilized to pay service provider bills. The invoices generated by the invoice component 1302 are output to the appropriate parties (*e.g.*, customer 102, end user(s), or third parties) at reference number 1514. Invoices can be communicated by any appropriate means, including, but not limited to, email, electronic transfer, or printed and delivered by mail.

[000120] FIG. 16 is a flowchart that depicts an exemplary methodology for configuring the device management system 100 for a customer 102. At reference number 1602, the business requirements of the particular customer 102 are gathered. Such requirements include procurement requirements (*e.g.*, available service providers, devices and service plans) support requirements (*e.g.*, twenty-four hour replacement guaranteed), invoicing or billing requirements (*e.g.*, division of charges based upon function, business unit or the like) and asset management (*e.g.*, description of reports desired by customer 102). Once the customer business requirements are defined, the mobile strategy for the particular customer 102 is established at reference number 1602. The strategy can include minimization of overall costs, distribution of costs over multiple business units. The strategy is composed of one or more priorities. The business requirements and strategies are determined based upon customer interviews, questionnaires, analysis of customer's business and hierarchy and any other customer information. The business requirements and strategy of customers are reflected in customer policies incorporated in the customer data store 204.

[000121] At reference number 1606, a customer profile and policies, maintained in the customer data store 204, are configured. In addition, the user interface 202 is updated and customized based at least in part upon customer policies and business requirements as obtained at reference numbers 1602 and 1604. The customized user interface 202 can enforce user policies by selectively restricting access to certain information and functionalities, and by selectively limiting options for election. Access and options may be restricted based upon user, position of user within the customer 102, length of service or any other characteristic as specified in user policies and practices.

[000122] Data regarding current users, mobile device, service plans and the like is loaded into the asset data store 214 at reference number 1608. Loading of data includes parsing data records maintained by the customer 102, extracting the data and storing the data in a standardized format utilized by the device management system 100. The customized user interface 202 is deployed at reference number 1610. Once deployed the user interface 202 is accessible to one or more users associated with the customer 102. In an embodiment, the user interface 202 is a centralized web portal that provides for access to one or more tools for managing mobile devices *via* the Internet.

[000123] After the user interface 202 is deployed, the customer 102 can utilize the user interface 202 to manage mobile devices. At 1612, the asset component 212 and/or optimization component 706 analyze the various service provider plans, usage and assets to determine excessive charges or defects that can be resolved to provide opportunities to reduce costs to the customer 102. In one embodiment, analysis and optimization occur when relationship between customer 102 and the device management system 100 is initiated. In another embodiment, analysis and optimization processes are continuous or periodic during the existence of the relationship between the customer 102 and the device management system 100. At 1614, recommendations or corrections for the defects are implemented. In general, recommendations will be approved by a representative of the customer 102. The approved recommendations can be implemented by notifying the appropriate service provider 104 and updating information in the asset data store 214.

[000124] At 1616, the recommendations or suggestions for optimization of mobile devices for a customer 102 can be improved by training the device management system 100. As recommendations are accepted or rejected, the device management system 100 learns preferred recommendations. In addition, the device management system 100 can evaluate and analyze the results of implemented recommendations to determine actual affect. In an embodiment, recommendations are weighted based upon projected affect. Weights can be determined from historical information, such as similar previously implemented recommendations.

[000125] Turning now to FIG. 17, a flowchart depicting an exemplary methodology for configuring the user interface 202 for a particular customer 102 is illustrated. At reference number 1702 the user interface 202 "click-path" is configured. As used herein, the click-path indicates the series of windows or screens with which a user interacts when utilizing the user

interface 102, typically by clicking or selecting on buttons on a display screen. Here, the click-path is customized as a function of the policies or requirements of the customer. For example, the customer may require the end user to select the business unit to which they belong before selecting the desired service provider on the following web page.

[000126] At reference number 1704, the virtual inventory is configured based upon user policies. Here, the virtual inventory is the inventory of available mobile devices from which an end user can order a mobile device. The particular devices presented as available through the user interface 202 are determined based upon user policies, and may vary based upon user position, business unit, title, or other characteristic. At 1706, data from service providers 104 is used to configure the user interface 202 and device management system 100 for the particular discounts, plans and services the customer 102 has negotiated with one or more service providers 104. Such discounts may affect options provided to users. In addition, such information is used to recommend optimizations.

[000127] At 1708, customized fields are added to the user interface 202 for collection of customer specific information. This ability to add fields to the user interface 202 provides the device management system 100 with significant flexibility. For example, nonstandard information can be collected by adding fields to the user interface 202. Introduction of customer specific codes allows customers to track unique or at least uncommon features.

[000128] At reference number 1710, the procurement order approval process is customized based upon customer policy. In an embodiment, the customer 102 specifies a multi-tier approval process. For example, end users are restricted in their elections at the user interface 202. Once the user has completed the order request, the generated order is provided to an administrator or other individual or department at the customer 102 with authority to approve the order. The request may be provided in any format suitable for use by the customer 102. In another embodiment, the approval process may be specific to the user placing the order. For example, the user's manager may be required to approve the order.

[000129] Additional customer specific information can be added to the user interface 202 at reference number 1712. In one embodiment, the customer 102 provides an Acceptable Use Policy (AUP) that dictates use of the user interface 202. In another embodiment, customer 102 may personalize instructions or other messages to users. At reference number 1714, information regarding the customer's business hierarchy is utilized to generate a model hierarchy. In particular, information regarding, departments, business units, site or locations

and the like are used to generate a model of the customer business. This model can be used in invoice or report generation to provide data in a manner that is useful for the customer 102.

[000130] At reference number 1716, a determination is made as to whether the user interface 202 will interact with an existing procurement system of the customer's (*e.g.*, Ariba) or whether the user interface 202 will operate as a stand-alone system. If the device management system 100 will interact with an existing procurement system, the user interface 202 is retrofitted to exchange information with the existing system at reference number 1718. Otherwise, at reference number 1720, the user interface 202 is deployed as an independent web portal.

[000131] The device management system 100 described herein can be implemented using various combinations of hardware and software. For example, the system 100 can be implemented using a microprocessor, microcontroller, or central processor unit (CPU) chip and printed circuit board (PCB). Alternatively, the system 100 can include an application specific integrated circuit (ASIC), programmable logic controller (PLC), programmable logic device (PLD), digital signal processor (DSP), or the like. In addition, the device management system 100 includes memory, whether static memory, such as erasable programmable read only memory (EPROM), electronically erasable programmable read only memory (EEPROM), flash or bubble memory, hard disk drive, tape drive or any combination of static memory and dynamic memory. The device management system 100 can utilize software and operating parameters stored in the memory. In addition, the user information can be implemented using various combinations of input and output devices, including, but not limited to, a monitor, keyboard, mouse, trackball or other pointer device.

[000132] While various embodiments have been described above, it should be understood that the embodiments have been presented by way of example only, and not limitation. It will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the subject matter described herein and defined in the appended claims. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

WE CLAIM:

1. A system that manages a plurality of mobile devices associated with a customer, comprising:

a customer data store that maintains customer data comprising a customer policy and end user data related to a plurality of end users associated with the customer;

a service provider data store that maintains service provider data associated with a plurality of service providers, said service provider data comprising at least one service plan offered by said plurality of service providers;

a user interface that provides said plurality of end users and the customer with an interface to the system; and

an aggregation component that utilizes said service provider data, said customer policy and said end user data to enable the customer to manage the plurality of mobile devices used by said plurality of end users.

2. The system of claim 1, further comprising a procurement component that obtains the plurality of mobile devices from said plurality service providers in accordance with said customer policy.

3. The system of claim 2, wherein said customer policy describes an approval process for procuring a mobile device.

4. The system of claim 3, wherein said customer policy further describes at least one available service associated with a subset of end users selected from said plurality of end users based, at least in part, upon a characteristic associated with each of said subset of end users.

5. The system of claim 1, further comprising a billing component that allocates cost associated with the plurality of mobile devices as a function of said customer policy.

6. The system of claim 5, whereby said cost from said service providers is partially allocated to the customer for said plurality of end users, with the remainder allocated to said plurality of end users based, at least in part, upon said at least one service plan provisioned for each of said plurality of end users.

7. The system of claim 5, said cost is allocated based at least in part upon a customer business unit.

8. The system of claim 5, further comprising:

an asset data store that maintains asset data corresponding to the plurality of mobile devices; and

a reconciliation component that reconciles said cost and usage data associated with the plurality of mobile devices with said customer data, said service provider data and said asset data, said cost and said usage data is obtained from said plurality of service providers.

9. The system of claim 8, further comprising a reporting component that generates an exception report detailing exceptions from said customer policy for each of said plurality of end users, based at least in part upon, said cost and said usage data associated with an individual end user selected from said plurality of end users.

10. The system of claim 1, wherein said customer data further comprises usage data that describes use characteristics of the plurality of mobile devices by said plurality of end users.

11. The system of claim 1, further comprising an optimization component that analyzes said customer data in conjunction with said service provider data and generates a recommendation for reducing cost associated with the plurality of mobile devices.

12. The system of claim 1, further comprising a support component adapted to facilitate support for said plurality of end users.

13. The system of claim 1, further comprising an asset component that provides the customer with ability to monitor provisioning and use of the plurality of mobile devices to said plurality of end users.

14. The system of claim 11, whereby a wireless number for each of the plurality of mobile devices is utilized as a device identifier for monitoring the plurality of mobile devices.

15. The system of claim 1, further comprising a means for transforming said customer data into a standardized format for data aggregation and import into an accounting system.

16. A method of managing a plurality of mobile devices for a customer, comprising:

obtaining customer data indicative of a customer policy, said customer policy related to the plurality of mobile devices;

obtaining end user data related to a plurality of end users associated with the customer;

obtaining service provider data associated a plurality of service providers;

deploying a user interface adapted to facilitate management of the plurality of mobile devices as a function of said customer policy, said service provider data and said end user data; and

generating a recommendation to improve management of the plurality of mobile devices in accordance with said customer policy, said end user data and said service provider data.

17. The method of claim 16, further comprising procuring at least one of the plurality of mobile devices *via* said user interface.

18. The method of claim 17, further comprising authorizing procurement of at least one of the plurality of mobile devices as a function of said customer policy.

19. The method of claim 16, further comprising generating an exception report that provides details of usage of at least one of the plurality of mobile devices, said exception report is indicative of a violation of said customer policy.

20. The method of claim 16, further comprising coordinating support of the plurality of mobile devices from said plurality of service providers for said plurality of end users.

21. The method of claim 16, further comprising allocating cost for the plurality of mobile devices based at least in part upon a service plan associated with each of the plurality of mobile devices.

22. The method of claim 16, further comprising allocating cost for the plurality of mobile devices based at least in part upon a characteristic of each of said plurality of end users.

23. The method of claim 16, further comprising invoicing an individual selected from said plurality of end users for cost associated with a mobile device selected from the plurality of mobile devices, said mobile device is assigned to said individual.

24. The method of claim 16, further comprising aggregating billing for said plurality of service providers.

25. A system for managing a plurality of mobile devices associated with a customer, comprising:

a customer data store comprising a customer policy defining procurement and provisioning preferences of the customer, and end user information pertaining to an end user associated with the customer, the end user information comprising an end user characteristic, an end user historical use data, and an end user provisioning history;

a service provider data store adapted to store service provider data associated with a plurality of service providers, said service provider data comprising a service plan and a mobile device selected from the plurality of mobile devices associated with said service plan;

a user interface adapted to interface with the customer, said user interface includes a means for updating said customer data store and a means for reporting details associated with said service provider data store and said customer data store;

means for providing procurement options to said customer, selected by applying said customer policy and said end user information to said service provider data, said procurement options are presented *via* said user interface;

means for procuring said mobile device from one of said plurality of service providers and said service plan from one of said plurality of service providers based at least in part upon input received from the customer via said user interface;

means for provisioning said mobile device that activates and provides said service plan and said mobile device to an end user;

means for processing an invoice from said plurality of service providers; and

means for updating said customer data store with details obtained from said invoice for the customer and updating said end user historical use data with details obtained from said invoice.

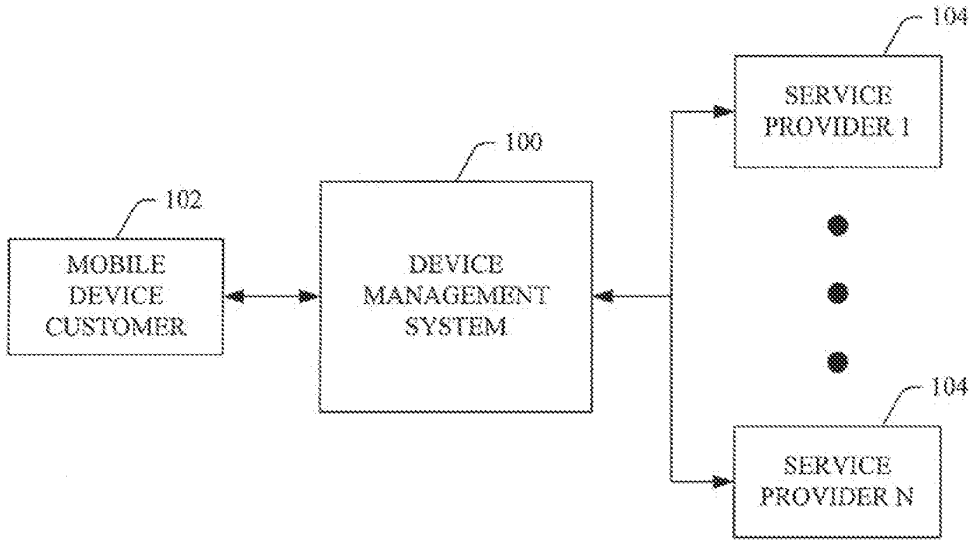

104
SERVICE PROVIDER 1
100
102
MOBILE DEVICE CUSTOMER
DEVICE MANAGEMENT SYSTEM
104
SERVICE PROVIDER N

FIG. 1

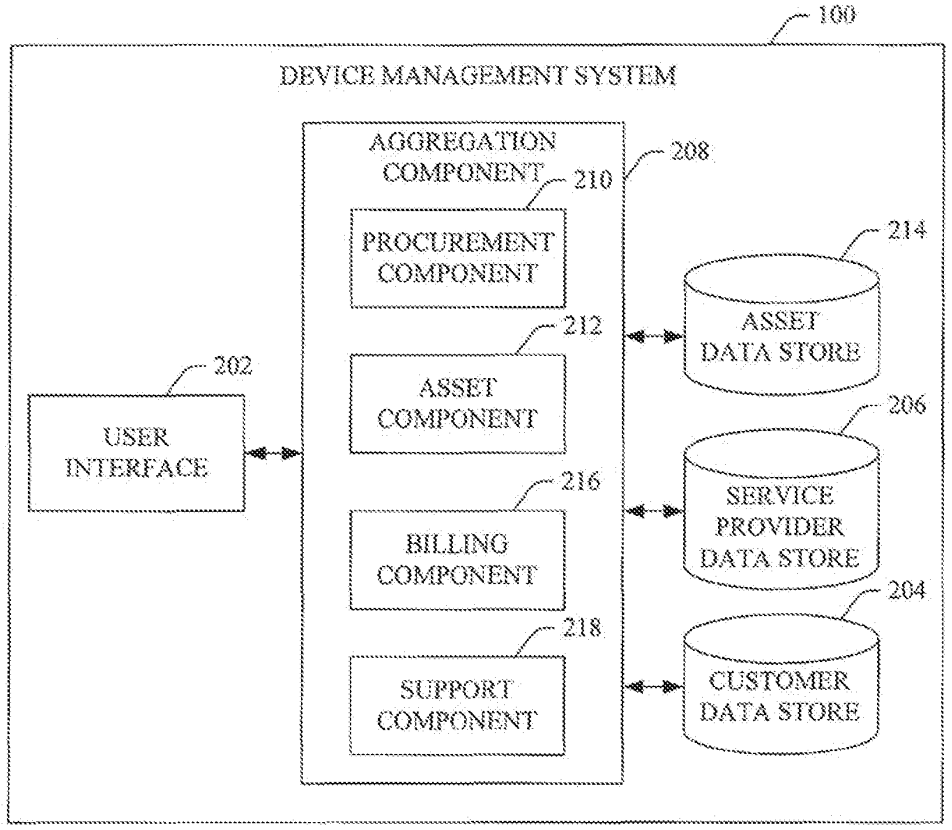

100
DEVICE MANAGEMENT SYSTEM
AGGREGATION COMPONENT
208
210
PROCUREMENT COMPONENT
212
ASSET COMPONENT
216
BILLING COMPONENT
218
SUPPORT COMPONENT
202
USER INTERFACE
214
ASSET DATA STORE
206
SERVICE PROVIDER DATA STORE
204
CUSTOMER DATA STORE

FIG. 2

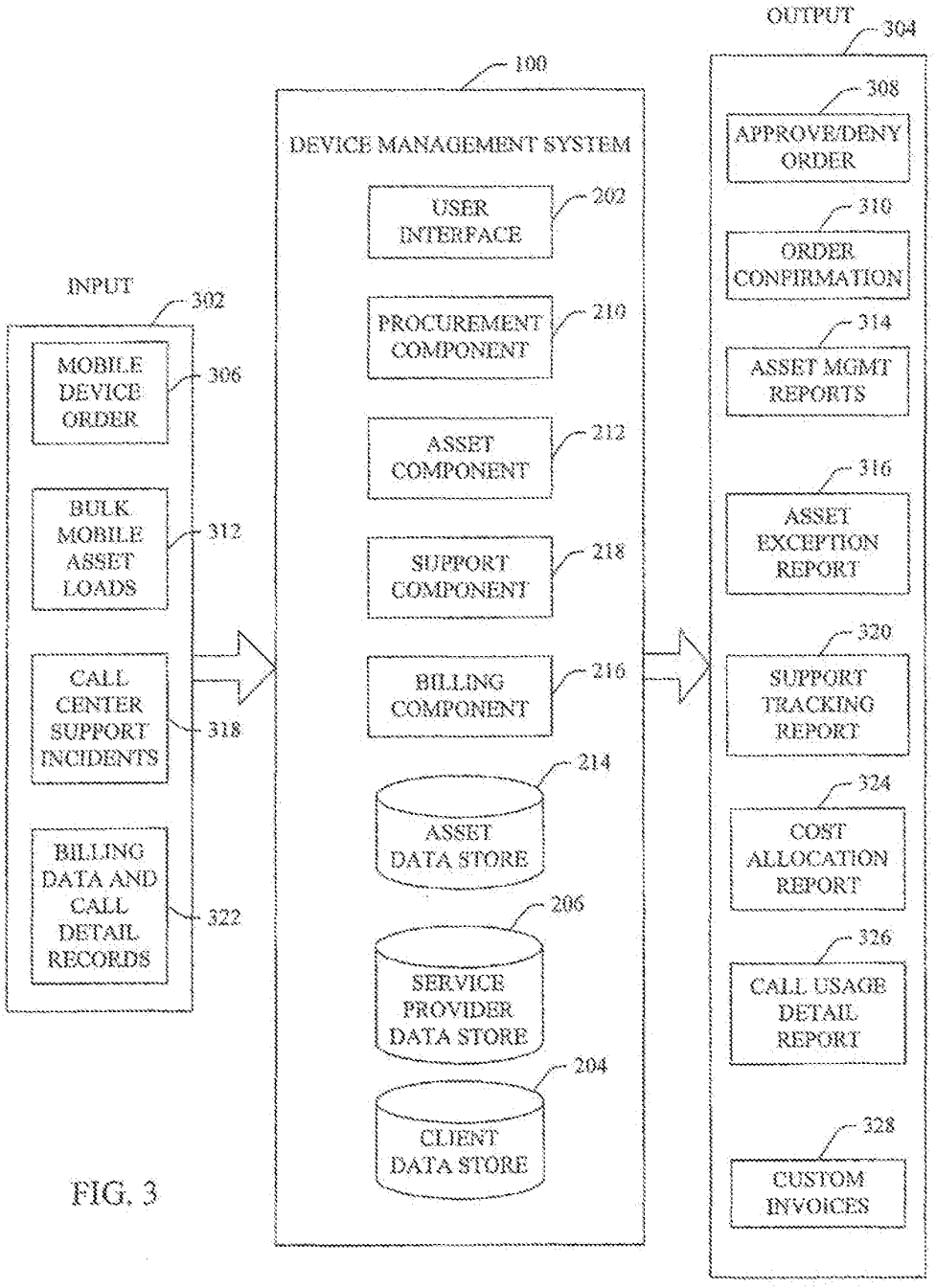

INPUT
302
MOBILE DEVICE ORDER
306
BULK MOBILE ASSET LOADS
312
CALL CENTER SUPPORT INCIDENTS
318
BILLING DATA AND CALL DETAIL RECORDS
322
100
DEVICE MANAGEMENT SYSTEM
USER INTERFACE
202
PROCUREMENT COMPONENT
210
ASSET COMPONENT
212
SUPPORT COMPONENT
218
BILLING COMPONENT
216
ASSET DATA STORE
214
SERVICE PROVIDER DATA STORE
206
CLIENT DATA STORE
204
OUTPUT
304
APPROVE/DENY ORDER
308
ORDER CONFIRMATION
310
ASSET MGMT REPORTS
314
ASSET EXCEPTION REPORT
316
SUPPORT TRACKING REPORT
320
COST ALLOCATION REPORT
324
CALL USAGE DETAIL REPORT
326
CUSTOM INVOICES
328

FIG. 3

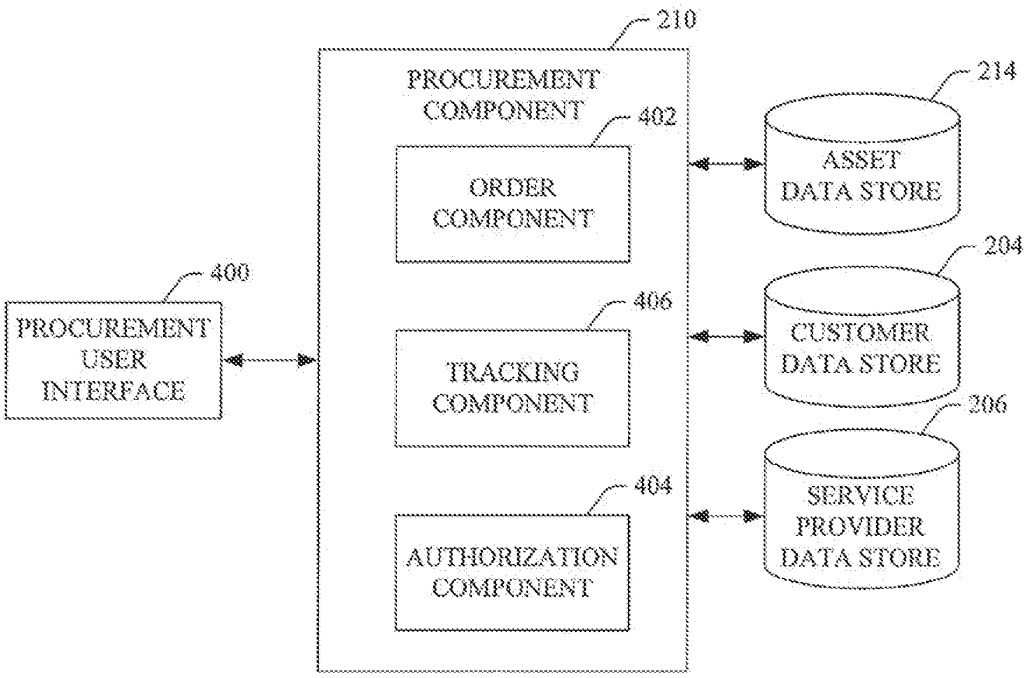

210
PROCUREMENT COMPONENT
402
ORDER COMPONENT
406
TRACKING COMPONENT
404
AUTHORIZATION COMPONENT
400
PROCUREMENT USER INTERFACE
214
ASSET DATA STORE
204
CUSTOMER DATA STORE
206
SERVICE PROVIDER DATA STORE

FIG. 4

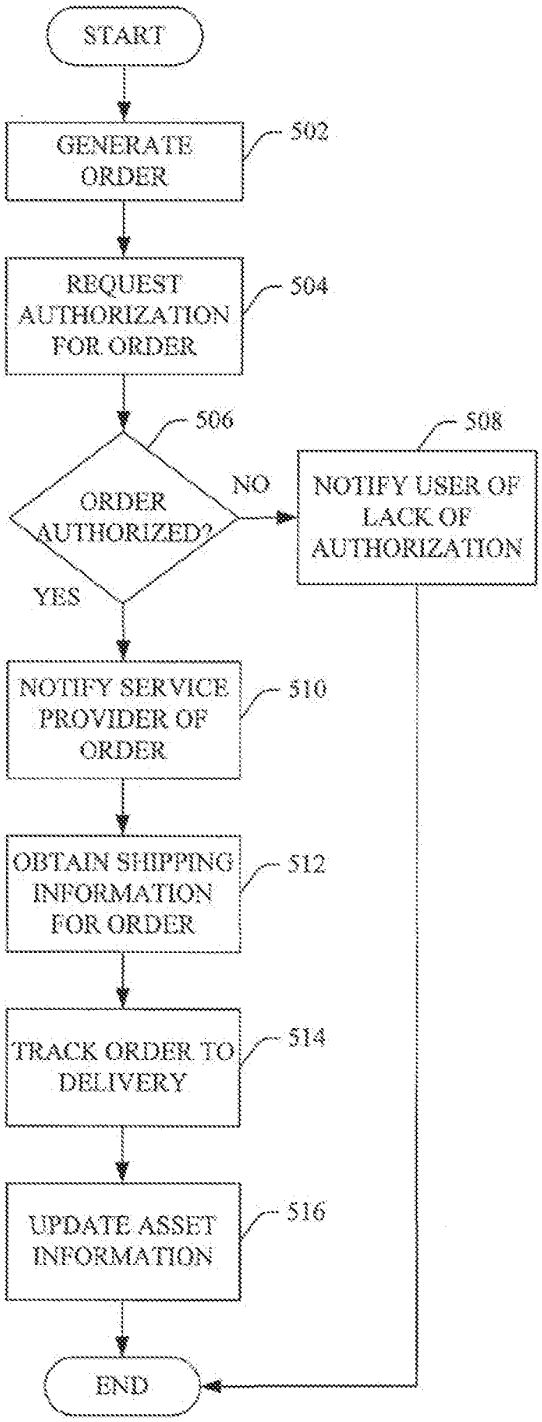

START
GENERATE ORDER
502
REQUEST AUTHORIZATION FOR ORDER
504
506
ORDER AUTHORIZED?
NO
508
NOTIFY USER OF LACK OF AUTHORIZATION
YES
NOTIFY SERVICE PROVIDER OF ORDER
510
OBTAIN SHIPPING INFORMATION FOR ORDER
512
TRACK ORDER TO DELIVERY
514
UPDATE ASSET INFORMATION
516
END

FIG. 5

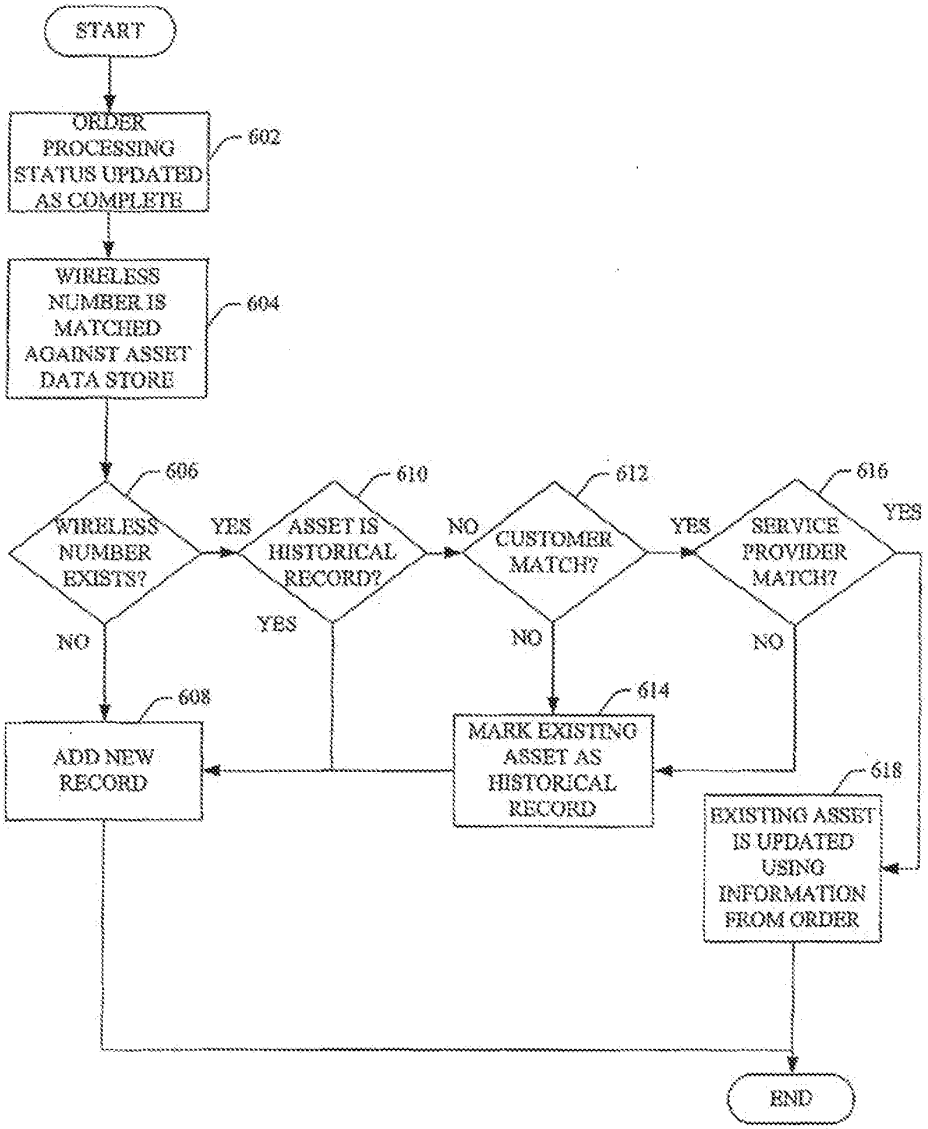

START
ORDER PROCESSING STATUS UPDATED AS COMPLETE
602
WIRELESS NUMBER IS MATCHED AGAINST ASSET DATA STORE
604
606
WIRELESS NUMBER EXISTS?
YES
610
ASSET IS HISTORICAL RECORD?
NO
612
CUSTOMER MATCH?
YES
616
SERVICE PROVIDER MATCH?
YES
NO
YES
NO
NO
608
ADD NEW RECORD
614
MARK EXISTING ASSET AS HISTORICAL RECORD
618
EXISTING ASSET IS UPDATED USING INFORMATION FROM ORDER
END

FIG. 6

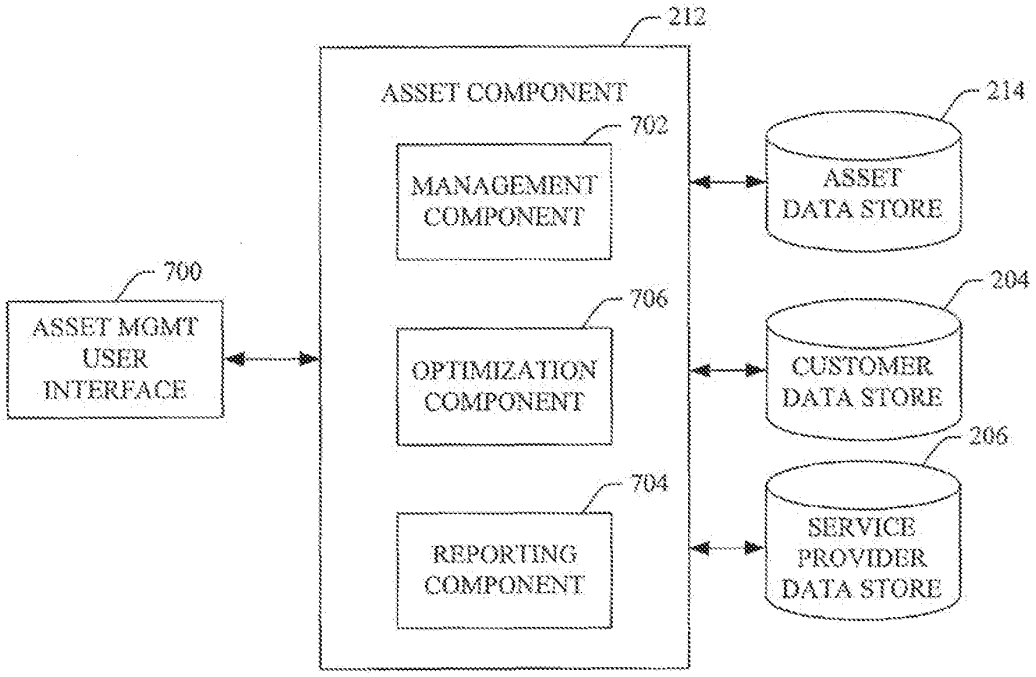

212
ASSET COMPONENT
702
MANAGEMENT COMPONENT
706
OPTIMIZATION COMPONENT
704
REPORTING COMPONENT
214
ASSET DATA STORE
204
CUSTOMER DATA STORE
206
SERVICE PROVIDER DATA STORE
700
ASSET MGMT USER INTERFACE

FIG. 7

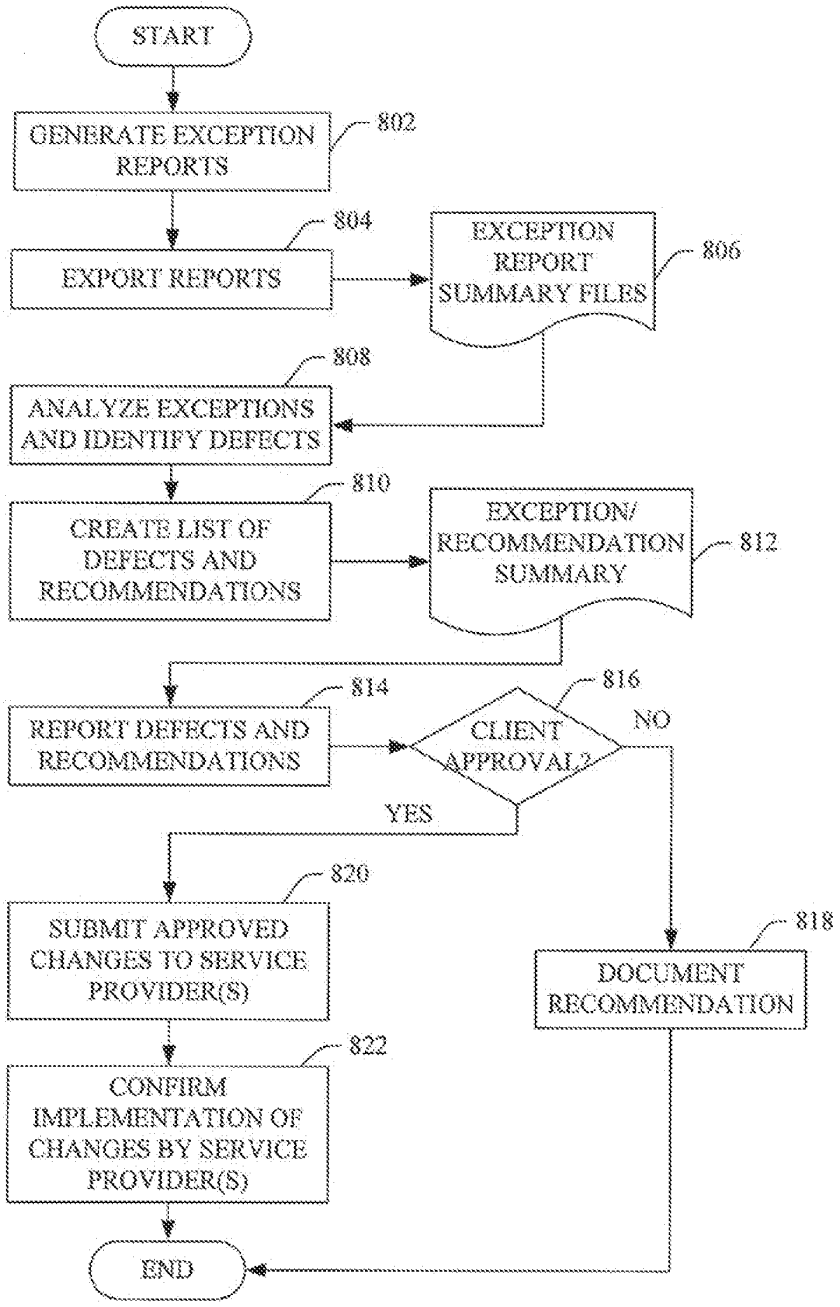

START
GENERATE EXCEPTION REPORTS
802
EXPORT REPORTS
804
EXCEPTION REPORT SUMMARY FILES
806
ANALYZE EXCEPTIONS AND IDENTIFY DEFECTS
808
CREATE LIST OF DEFECTS AND RECOMMENDATIONS
810
EXCEPTION/ RECOMMENDATION SUMMARY
812
REPORT DEFECTS AND RECOMMENDATIONS
814
CLIENT APPROVAL?
816
NO
YES
SUBMIT APPROVED CHANGES TO SERVICE PROVIDER(S)
820
DOCUMENT RECOMMENDATION
818
CONFIRM IMPLEMENTATION OF CHANGES BY SERVICE PROVIDER(S)
822
END

FIG. 8

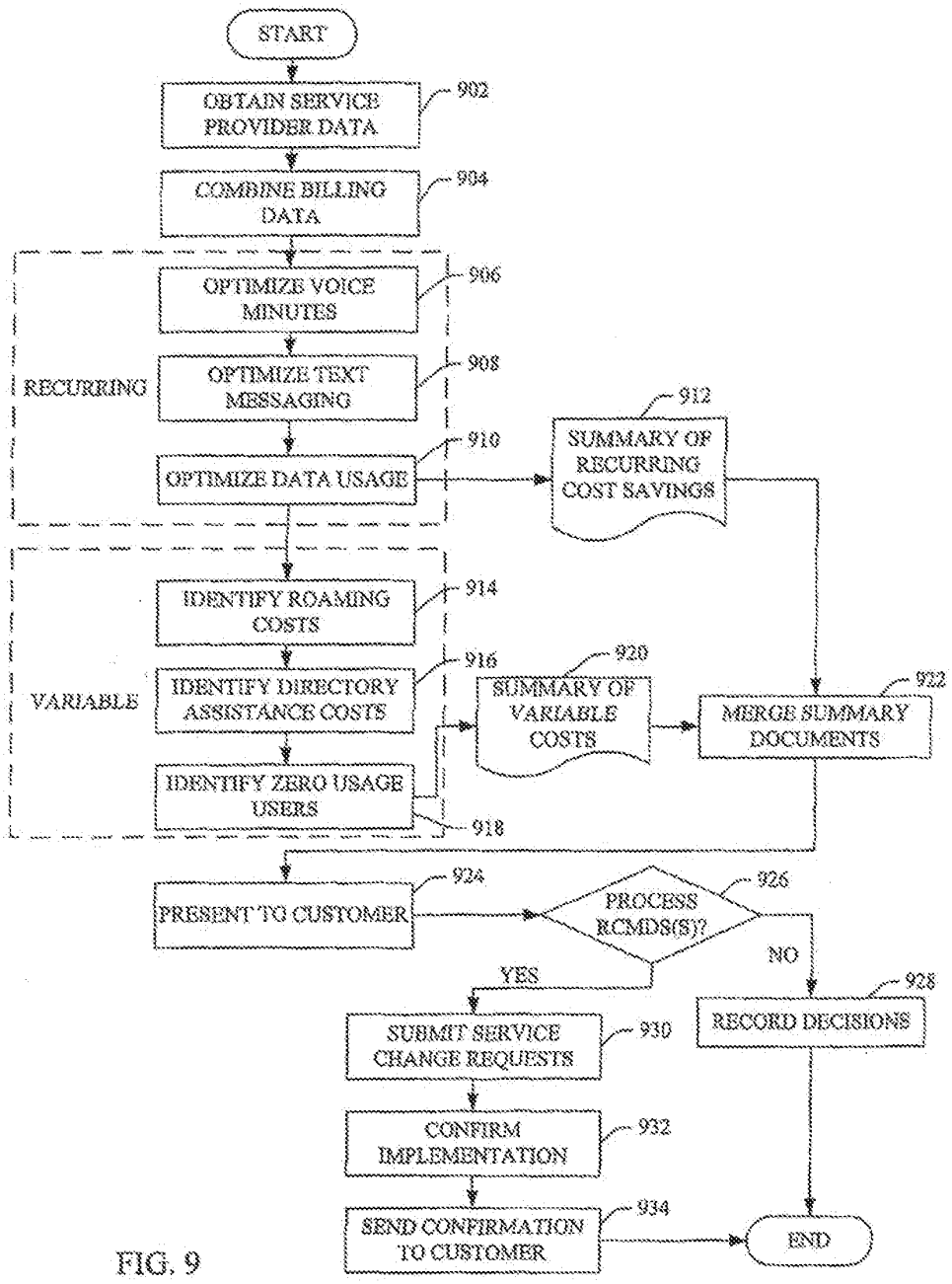

START
OBTAIN SERVICE PROVIDER DATA
902
COMBINE BILLING DATA
904
RECURRING
OPTIMIZE VOICE MINUTES
906
OPTIMIZE TEXT MESSAGING
908
OPTIMIZE DATA USAGE
910
SUMMARY OF RECURRING COST SAVINGS
912
VARIABLE
IDENTIFY ROAMING COSTS
914
IDENTIFY DIRECTORY ASSISTANCE COSTS
916
IDENTIFY ZERO USAGE USERS
918
SUMMARY OF VARIABLE COSTS
920
MERGE SUMMARY DOCUMENTS
922
PRESENT TO CUSTOMER
924
PROCESS RCMDS(S)?
926
YES
NO
SUBMIT SERVICE CHANGE REQUESTS
930
RECORD DECISIONS
928
CONFIRM IMPLEMENTATION
932
SEND CONFIRMATION TO CUSTOMER
934
END

FIG. 9

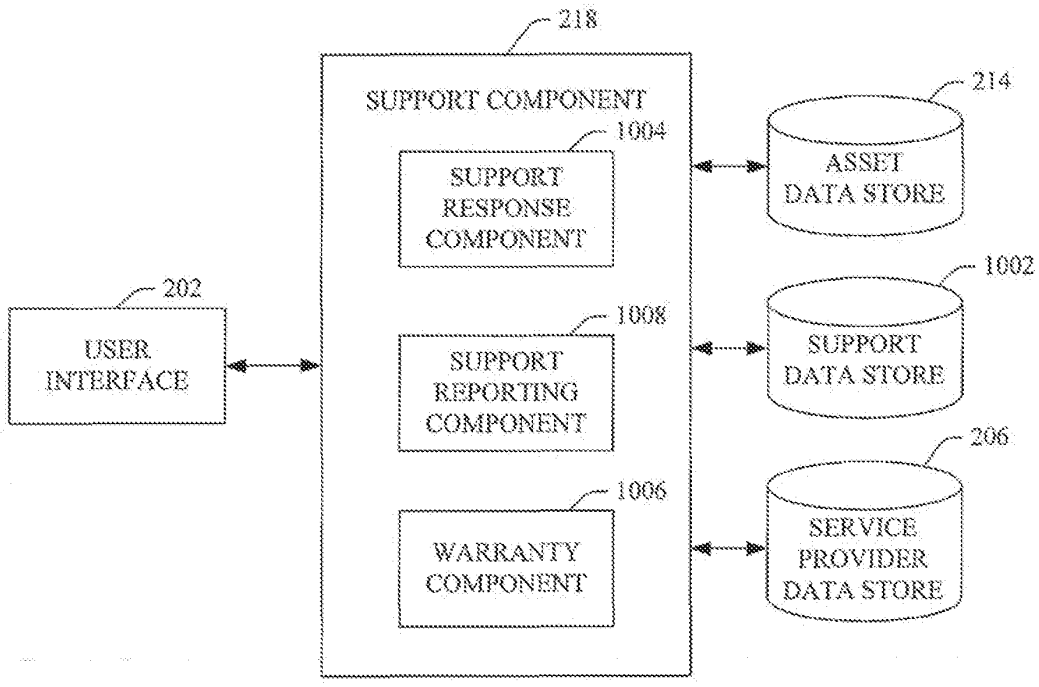

218
SUPPORT COMPONENT
1004
SUPPORT RESPONSE COMPONENT
1008
SUPPORT REPORTING COMPONENT
1006
WARRANTY COMPONENT
202
USER INTERFACE
214
ASSET DATA STORE
1002
SUPPORT DATA STORE
206
SERVICE PROVIDER DATA STORE

FIG. 10

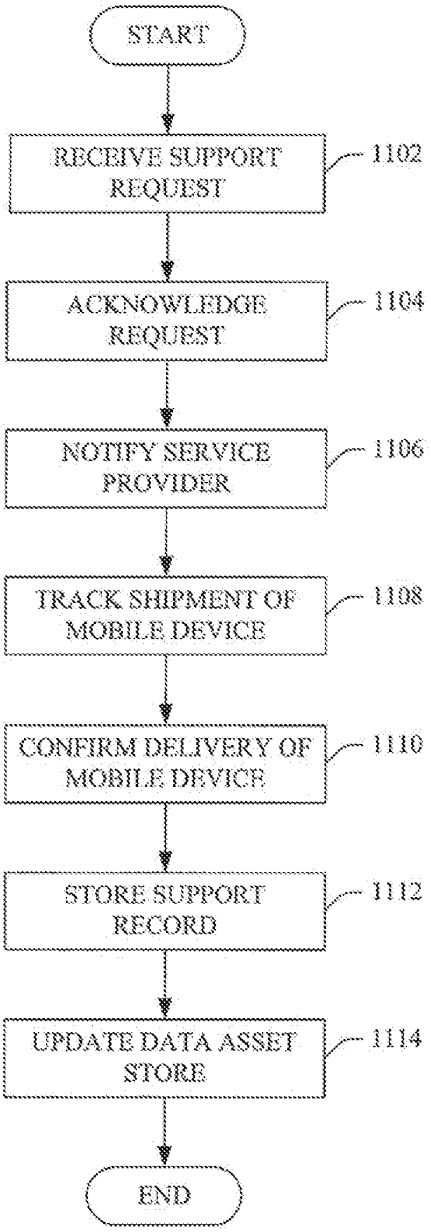

START
RECEIVE SUPPORT REQUEST
1102
ACKNOWLEDGE REQUEST
1104
NOTIFY SERVICE PROVIDER
1106
TRACK SHIPMENT OF MOBILE DEVICE
1108
CONFIRM DELIVERY OF MOBILE DEVICE
1110
STORE SUPPORT RECORD
1112
UPDATE DATA ASSET STORE
1114
END

FIG. 11

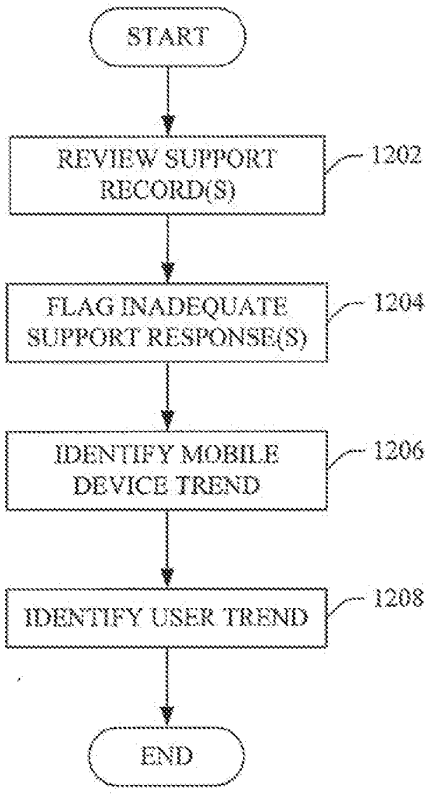

START
REVIEW SUPPORT RECORD(S)
1202
FLAG INADEQUATE SUPPORT RESPONSE(S)
1204
IDENTIFY MOBILE DEVICE TREND
1206
IDENTIFY USER TREND
1208
END

FIG. 12

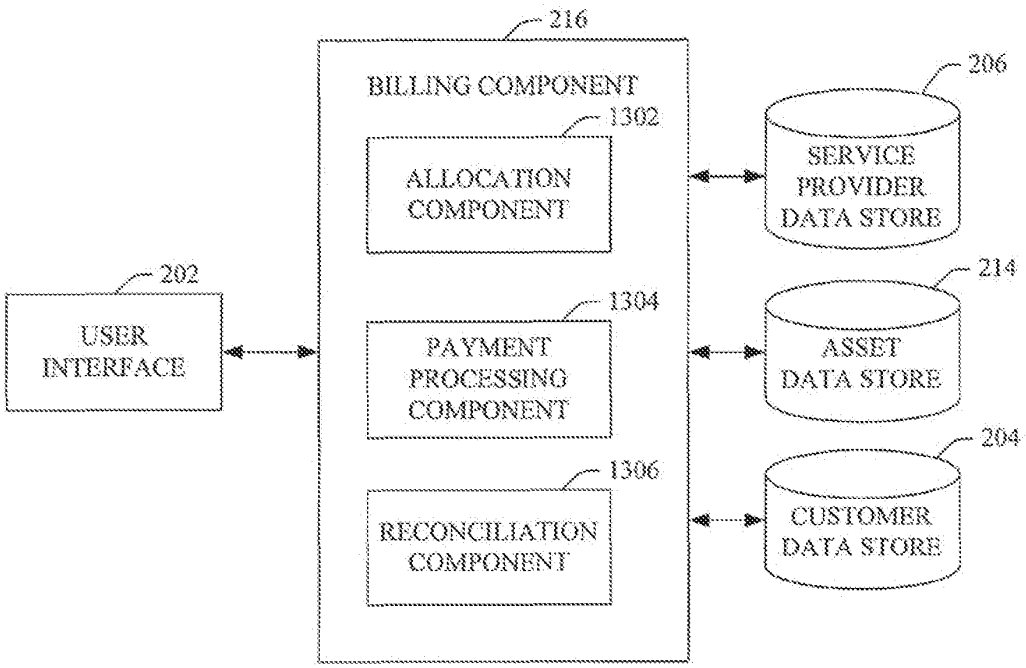

216
BILLING COMPONENT
1302
ALLOCATION COMPONENT
1304
PAYMENT PROCESSING COMPONENT
1306
RECONCILIATION COMPONENT
202
USER INTERFACE
206
SERVICE PROVIDER DATA STORE
214
ASSET DATA STORE
204
CUSTOMER DATA STORE

FIG. 13

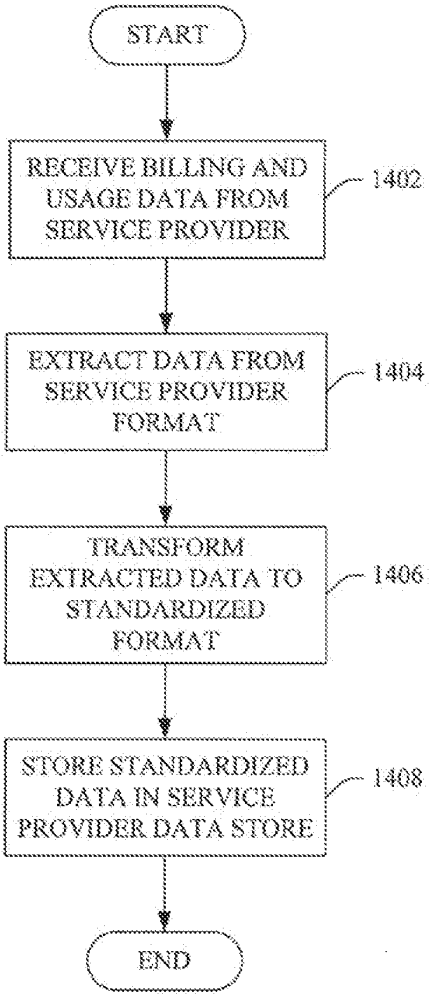

START
RECEIVE BILLING AND USAGE DATA FROM SERVICE PROVIDER
1402
EXTRACT DATA FROM SERVICE PROVIDER FORMAT
1404
TRANSFORM EXTRACTED DATA TO STANDARDIZED FORMAT
1406
STORE STANDARDIZED DATA IN SERVICE PROVIDER DATA STORE
1408
END

FIG. 14

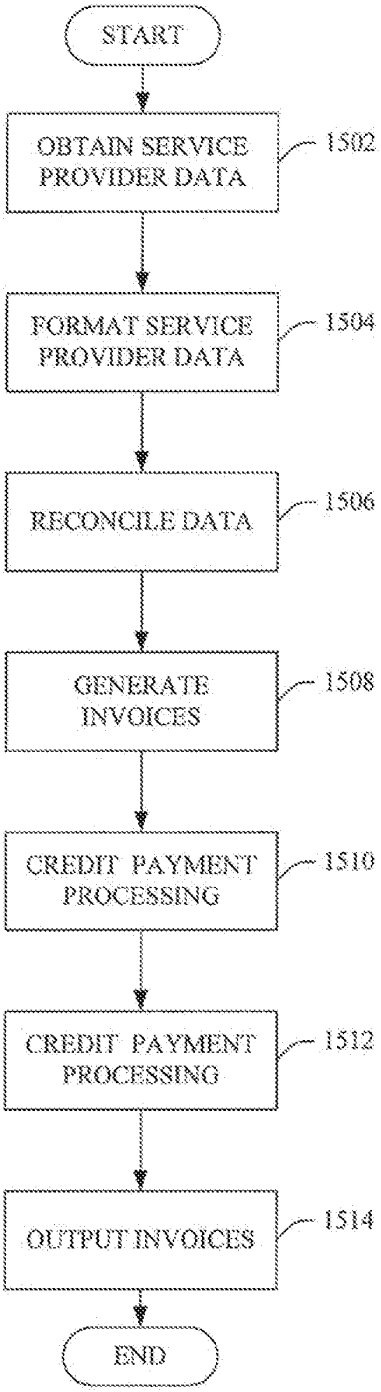

START
OBTAIN SERVICE PROVIDER DATA
1502
FORMAT SERVICE PROVIDER DATA
1504
RECONCILE DATA
1506
GENERATE INVOICES
1508
CREDIT PAYMENT PROCESSING
1510
CREDIT PAYMENT PROCESSING
1512
OUTPUT INVOICES
1514
END

FIG. 15

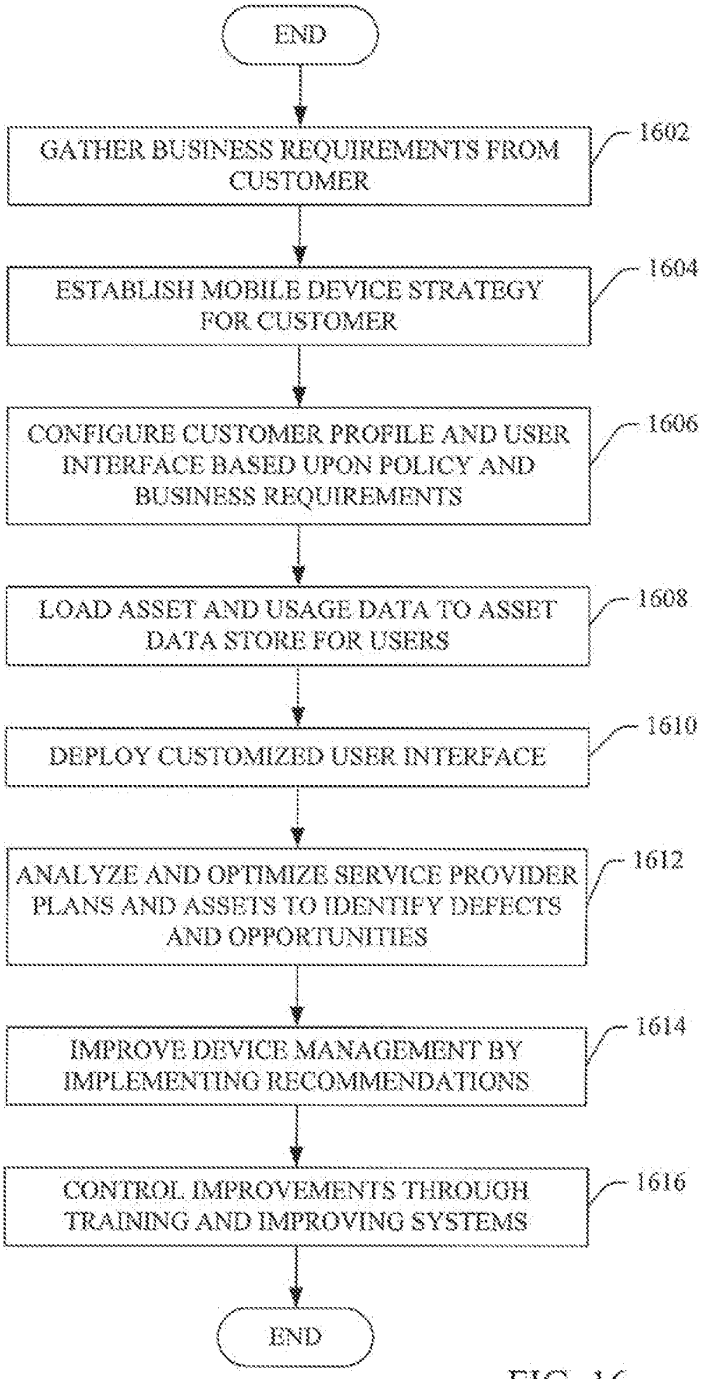

END
GATHER BUSINESS REQUIREMENTS FROM CUSTOMER
1602
ESTABLISH MOBILE DEVICE STRATEGY FOR CUSTOMER
1604
CONFIGURE CUSTOMER PROFILE AND USER INTERFACE BASED UPON POLICY AND BUSINESS REQUIREMENTS
1606
LOAD ASSET AND USAGE DATA TO ASSET DATA STORE FOR USERS
1608
DEPLOY CUSTOMIZED USER INTERFACE
1610
ANALYZE AND OPTIMIZE SERVICE PROVIDER PLANS AND ASSETS TO IDENTIFY DEFECTS AND OPPORTUNITIES
1612
IMPROVE DEVICE MANAGEMENT BY IMPLEMENTING RECOMMENDATIONS
1614
CONTROL IMPROVEMENTS THROUGH TRAINING AND IMPROVING SYSTEMS
1616
END

FIG. 16

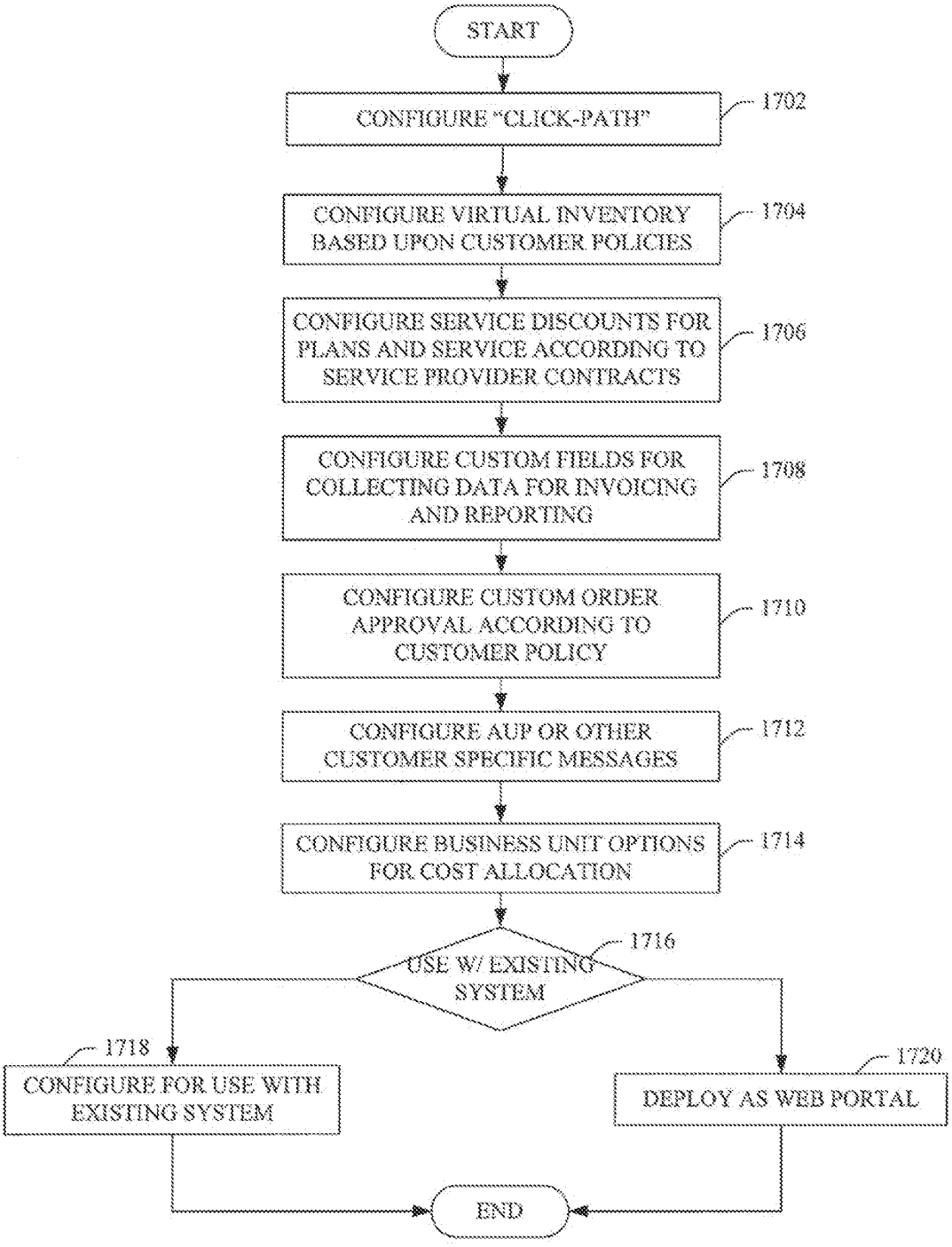

START
CONFIGURE "CLICK-PATH"
1702
CONFIGURE VIRTUAL INVENTORY BASED UPON CUSTOMER POLICIES
1704
CONFIGURE SERVICE DISCOUNTS FOR PLANS AND SERVICE ACCORDING TO SERVICE PROVIDER CONTRACTS
1706
CONFIGURE CUSTOM FIELDS FOR COLLECTING DATA FOR INVOICING AND REPORTING
1708
CONFIGURE CUSTOM ORDER APPROVAL ACCORDING TO CUSTOMER POLICY
1710
CONFIGURE AUP OR OTHER CUSTOMER SPECIFIC MESSAGES
1712
CONFIGURE BUSINESS UNIT OPTIONS FOR COST ALLOCATION
1714
USE W/ EXISTING SYSTEM
1716
1718
CONFIGURE FOR USE WITH EXISTING SYSTEM
1720
DEPLOY AS WEB PORTAL
END

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 07/88732

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04J 3/14 (2008.01)
USPC - 370/230
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8)- H04J 3/14 (2008.01)
USPC-370/230

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC-370/230, 230.1

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWest (USPT, PG, PB, EPAB, JPAB); DialogPRO (Engineering); Google Scholar
Search Terms Used: mobile device, client data, customer data, user interface, sum, aggregation, management system, service provider

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2004/0005873 A1 (Groenendaal et al.) 08 January 2004 (08.01.2004) (abstract)(para [0011], [0034], [0036], [0038], [0041], [0052], [0054], [0062]-[0063], [0065])	1,15-16, 22, 24 2-14, 17-21, 23, 25
Y	US 2006/0036520 A1 (O'Neill) 16 February 2006 (16.02.2006) (para [0001], [0004], [0012]-[0014], [0018], [0020], [0024], [0043], [0056])	2-14, 17-21, 23, 25

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 April 2008 (11.04.2008)	01 MAY 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2007)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 September 2004 (10.09.2004)

PCT

(10) International Publication Number
WO 2004/077797 A2

(51) International Patent Classification⁷: H04M

(21) International Application Number: PCT/US2003/005252

(22) International Filing Date: 23 February 2003 (23.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/449,907 25 February 2003 (25.02.2003) US

(71) Applicant (*for all designated States except US*): **BOSTON COMMUNICATIONS GROUP, INC.** [US/US]; 100 Sylvan Road, Suite 100, Woburn, MA 01801 (US).

(72) Inventors: **ERSKINE, Thomas**; 15 Summit Road, Marblehead, MA 01845 (US). **SONBERG, Kenneth, W.**; 6 Greyhirch Road, Andover, MA 01810 (US). **RUDISILL, Luther**; 6804 Poco Drive, Parker, TX 75002 (US).

(74) Agents: **LEBOVICI, Victor, B.** et al.; Weingarten, Schurgin, Gagnebin & Lebovici, LLP, Ten Post Office Square, Boston, MA 02109 (US).

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

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

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designation: US*

Published:

— *without international search report and to be republished upon receipt of that report*

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

(54) Title: METHOD AND SYSTEM FOR PROVIDING SUPERVISORY CONTROL OVER WIRELESS PHONE USAGE

(57) Abstract: A system for controlling wireless phone usage enables a supervisor to establish user profiles for supervised users of wireless phones across a range of parameters which are stored in a user profile database. Such parameters may include one or more locations at which use of the wireless phone is restricted or permitted. In addition, restrictions on phone use may be provided based upon total phone usage within a specified control period, time periods, dates or days of the week during which phone use is restricted or permitted. One or more lists including numbers that are always-accessible may be provided and one or more lists including numbers that are never-accessible may also be provided. In the event a call does not satisfy predefined criteria, the call is blocked. Predetermined messages may be played to the called or calling party as applicable when a call is blocked. Boolean combinations of restrictions and permissive use criteria for the wireless phone may be specified to provide for flexibility when establishing use criteria for the wireless phone.

WO 2004/077797 A2

TITLE OF THE INVENTION
METHOD AND SYSTEM FOR PROVIDING SUPERVISORY CONTROL OVER WIRELESS PHONE USAGE

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims priority under 35 USC §119(e) to provisional application serial number 60/449,907, entitled "METHOD AND SYSTEM FOR EXERCISING SUPERVISORY CONTROL OVER WIRELESS PHONE USAGE", filed February 25, 2003.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

N/A

BACKGROUND OF THE INVENTION

The present invention generally relates to wireless communication systems and more specifically to a method and system for providing supervisory control over wireless phone usage.

Wireless phones are widely used in this country. Wireless phone service providers typically allow a wireless phone subscriber to place calls at any time. For reasons of safety and convenience, more and more parents are inclined to have their children of school age carry wireless phones to make it easier for their children to contact them and vice versa. It has also been observed, however, that many children that are provided wireless phones tend to spend inordinate amounts of time on calls to friends during the school day and late into the evenings, and that the availability of wireless phones can present a distraction during the school day. Presently available wireless phone systems provide no way to adequately

provide supervisory control of wireless phone usage by others, e.g. children.

Accordingly, it would be desirable to have a method and system by which supervisory control may be exercised over wireless phone usage. It would further be desirable to be able to establish a user profile for wireless phone service on a user by user basis without intervention by the telephone service provider. Moreover, it would be desirable to be able to have the ability to allow a supervisor to modify the user profile as circumstances warrant without requiring human intervention by the telephone service provider so as to allow a supervisor to readily change the nature of the wireless service available to supervised individuals.

BRIEF SUMMARY OF THE INVENTION

In accordance with the present invention, a method and system for exercising supervisory control over wireless phone usage is disclosed. The disclosed system allows a Supervisor, such as a parent or manager, to establish individual profiles for supervised Users of respective wireless phones across a range of parameters. For example, a parent may establish user profiles for each child that is to be provided a wireless phone. The user profiles allow the use of the respective phones by the child subject to controls on incoming and/or outgoing calls as specified by the Supervisor. For example, the disclosed system allows the Supervisor to limit the total phone usage time within a specified control period, such as a week or a month, to a predetermined number of minutes and, to prevent incoming or outgoing calls during specified periods, such as school hours, except from predetermined numbers (always accessible numbers) specified by the Supervisor. Restrictions on phone usage may also be defined with regard to incoming or outgoing calls while the phone is at or near defined geographic

locations. For example, calls may be blocked while the phone is within the grounds of a school attended by the user. Additionally, a location restriction may be employed in conjunction with other restrictions on phone use and capabilities described herein. For example, calls may be restricted if the wireless phone is at a prescribed geographic location and the time is within a time period specified by the Supervisor. More specifically, the decision whether to block or permit a call may be made as a Boolean function of any of the applicable restrictive or permissive criteria applicable to phone usage herein described. The location of the wireless phone may be obtained using cell sector identifiers alone or in combination with signal strength information, a global positioning system receiver disposed within the wireless phone or any other suitable technique for resolving the geographic location of the wireless phone.

In one embodiment, calls to predetermined numbers specified by the Supervisor, and time spent on calls from one or more numbers specified by the Supervisor, are not counted toward the total number of minutes permitted during the specified control period.

When a supervised user attempts to make a call during a period in which use is prohibited, a message may be played to the user indicating that the call will not go through at the specified time. Similarly, when a call is placed to a supervised user during a period in which wireless phone usage is prohibited, an audible message may be played to the calling party indicating that the phone is not accessible at the present time.

The Supervisor may also specify telephone numbers within the user profile that are never permitted to be connected to the respective user's phone, and the system will prevent calls from such numbers from being connected to the respective

wireless phone. Additionally, the system may prevent the wireless phone from being used to call predetermined numbers specified by the Supervisor. The numbers telephone that cannot be called from the supervised phone and the telephone numbers of phones from which communications are blocked are referred to herein as never-accessible numbers.

If voicemail capability is enabled for the respective user's phone, voicemail messages from callers other than always-accessible callers may optionally be blocked during periods when phone use is restricted.

Certain numbers, namely the always accessible numbers, may be identified within the user profile and callers from these numbers may always access the supervised wireless phone or voicemail should the phone not be answered, even during a prohibited use period. For example, a parent's home number or wireless phone number may be included in the profile so that the parent is always able to reach the child's phone. In the event the child or wireless phone user is not available when a call from such a number comes in, the call may be forwarded to voicemail if voicemail is enabled for that user. An incoming call to a supervised phone is analyzed to determine if the calling number is one of the numbers on the list of always-accessible numbers. If the calling number is not one of the numbers on the always-accessible list, the call will not go through during a prohibited use period. However, a caller is provided the ability to access the supervised wireless phone upon dialing of a security code referred to herein as a cut-through code. Thus, the Supervisor, (or an individual having knowledge of the cut-through code) may access the supervised wireless phone when calling from a number other than one of the always-accessible numbers via the use of the cut-through code.

The user profiles are maintained within a database that may be modified at any time by the Supervisor. More

specifically, the Supervisor can log in over a global communications network, or other network that permits remote access, and can change usage limits in real time, change, add, delete numbers that are always or never accessible to/by a particular supervised wireless phone, change restricted use times, and make all other permitted changes to the respective user profiles. To assure that changes to the respective user profiles managed by the Supervisor may be made only by the Supervisor, a security code is required to be entered and verified before permitting changes to be made to the managed user profiles under the respective Supervisor's control. The presently described supervisory functions may operate independent of billing controls such as real-time pre-paid billing controls, or post-paid billing systems, that may also be applicable to the respective supervised phone, although the information defining the restrictions on phone use may be stored in a separate database or a common database with billing parameters. Alternatively, the presently described functionality may be provided as an overlay to pre-paid billing controls or other call billing and control systems and may be configured to share resources with such other systems while exercising call control independently of such other systems. The presently described supervisory system may employ one or more servers that operate independent of servers that provide billing functionality, or alternatively, the presently described supervisory system may share server resources while exercising control independent of restrictions pertaining to billing functions.

Other aspects, features and advantages of the presently disclosed system for exercising supervisory control over wireless phone usage will be apparent from the Detailed Description of the Invention that follows.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

The invention will be more fully understood by reference to the following detailed description of the invention in conjunction with the drawings, of which:

Fig. 1 is a block diagram depicting a system operative in accordance with the present invention;

Fig. 2 is another block diagram depicting a system operative in accordance with the present invention;

Fig. 3 is a flow chart depicting the processing of incoming calls;

Fig. 4 is a flow chart depicting the processing of incoming calls;

Fig. 5 is a flow chart depicting the processing of outgoing calls; and

Fig. 6 is a flow chart depicting the processing of outgoing calls.

DETAILED DESCRIPTION OF THE INVENTION

U.S. provisional patent application serial number 60/449,907, entitled "METHOD AND SYSTEM FOR EXERCISING SUPERVISORY CONTROL OVER WIRELESS PHONE USAGE", filed February 25, 2003, is hereby incorporated herein by reference.

In accordance with the present invention, a system and method for providing Supervisory control over wireless phone usage is disclosed. Referring to Fig. 1, a Supervisor S1 10, such as a parent or manager, is provided the ability to define a user profile for each of one or more users, such as children or employees. The user profile includes parameters and information that are used to manage phone usage. For example, the user profile may specify the total number of minutes the supervised phone may be used during a specified control period, the time of day and/or day of week when incoming and/or outgoing calls are prohibited, telephone numbers for numbers

that are never accessible, and telephone numbers that are always accessible via the respective supervised phone, among other controlled characteristics.

Referring to Fig. 1, each wireless phone, shown for purposes of illustration as P1 12 and P2 14, may communicate with a wireless switch 16. For purposes of explanation, the wireless switch 16 in the illustrative embodiment may be a switch that is associated with a respective home serving system. The wireless switch 16 is communicably coupled to a Mobile Services Switching Center (MSC) 18 within a Service Switching Point SSP 1 20, which, in turn, is communicably coupled with the presently disclosed Supervisory Control System 22 via a telecommunications network 25 which typically includes a plurality of Signal Transfer Points (STPs) 26a, 26b, 26c, 26d, as known in the art.

The Supervisory Control System 22 includes a Service Control Point (SCP) 24 that communicates with the telecommunications network 25 and performs SS7 signaling, a Service Data Point (SDP) 30 that includes a User Profile Database 32 for storing a user profile associated with each supervised wireless phone subscribed to the presently disclosed service, and Business Logic 34 that serves as an intelligent interface between the SCP 24 and the User Profile Database 32. The Business Logic 34 typically comprises a computer that executes software to provide the supervisory processes herein described. The Supervisory Control System 22 further includes a Web-Server 36 that permits accounts to be established in the User Profile Database 32 and updated by Supervisor S1 10 as subsequently discussed. The Supervisory Control System 22 in the illustrated embodiment also includes a co-located Intelligent Peripheral or VRU 38 that is operative to play audible scripts in response to controls issued by the SDP 30. The VRU 38 may alternatively be located geographically

proximate to the respective SSP 20 as is known in the art. The SCP 24, Web-Server 36, SDP 30 and VRU 38 in the illustrated embodiment are communicably coupled via a local area network (LAN) 40, such as an Ethernet or any other suitable network. The SCP 24 employs SS7 signaling over the telecommunications network 25 and the SDP 30 executes control software to implement the supervisory control functions herein described.

The Supervisor S1 10, operating through a PC, mobile phone or other Internet enabled access point 42 equipped with a suitable browser or micro-browser, may access the Web-Server 36 via the Internet 28 or another suitable network to establish and modify user profiles for the respective Users U1 44, U2 46.

Control and operation of the presently disclosed Supervisory Control System 22 falls within several areas of functionality, which are listed below:

1. Supervisory Control System service subscription and provisioning.

2. User profile configuration

3. Event control

These functional capabilities are discussed in greater detail below.

1. Supervisory Control System Service Subscription and Provisioning

Further with reference to Fig. 1, the Supervisor S1 10 may create an Supervisory Control System account by accessing the Web-Server 36 within the Supervisory Control System 22 via the Access point 42 or alternatively, by calling a service representative who enters the applicable account information. A supervisory account identifier is associated with the respective Supervisory Control System account and stored in the

User Profile Database 32. Account setup includes the following three functions:

1. provisioning the Supervisory Control System account within the wireless network;

2. provisioning the Supervisory Control System account within the billing system so that appropriate charges will be applied with respect to each wireless supervised phone; and

3. establishing applicable Supervisory Control System parameters for each supervised wireless phone.

More specifically, when creating a Supervisory Control System account via a graphical user interface provided through the Web-Server 36, the Supervisor S1 10 may employ a browser resident on the access point 42 to access Web pages served by the Web-Server 36 within the Supervisory Control System 22 or alternatively, the Supervisor S1 10 may place a voice call to a service representative who enters applicable Supervisory Control System account information.

When creating a Supervisory Control System account via the Internet, the Web-Server 36 is accessed via a domain-name associated with a carrier and linked to the respective Web-Server 36. The interface provided by the Web-Server 36 guides the Supervisor S1 10 through the necessary steps to establish a Supervisory Control System account via one or more interface screens served by the Web-Server 36. Any suitable format for interface screens may be used as is appropriate for a given implementation, so long as the interface allows the Supervisor S1 10 to establish a Supervisory Control System account and to enter User Profile data applicable to one or more supervised phones.

After accessing the Web-Server 36, the Supervisor S1 10 may log in via the access point 42 using a conventional login registration process. During this login process, the Supervisor S1 10 typically provides a user name and an email

address. In response, the Web-Server 36 emails a pass code to the specified email address. The Supervisor S1 10 then enters the pass code into an interface screen served by the Web-Server 36 to confirm that the Supervisory Control System account is associated with the proper individual. The supervisory account identifier is associated with the Supervisory Control System account established by the Supervisor.

2. User Profile Configuration

Following the creation of a Supervisory Control System account as described above, the phones to be supervised through the account, are identified to the SSP 1 20 so that a determination can be made whether calls relating to such phones should be processed by the Supervisory Control System 22. Accordingly, the Supervisor S1 10 is requested by the Web-Server 36 to enter a logical phone identifier (which is referred to herein as a Mobile Station Identifier (MSID)) and the Electronic Serial Number (ESN) for each wireless phone in the Supervisory Control System account. The specific Mobile Station Identifier employed may vary from system to system. For example, the MSID may be a Mobile Directory Number (MDN), a Mobile Identification Number (MIN), an International Mobile Subscriber Identity (IMSI) or a Mobile Subscriber International Services Directory Number (MSISDN) or any other suitable phone identifier. In the illustrative example, the MSID and the ESN for wireless phones P1 12 and P2 14 shown in Fig. 1, that are to be supervised by the respective Supervisor S1 10, are associated with the Supervisory Control System account. The Supervisor S1 10 also associates the name of each user with the applicable identifier(s) for the respective wireless phones. For example, in the illustrative configuration shown in Fig. 1, the Supervisor S1 10 would enter the name of User 1 U1 44 in association with wireless phone P1 12, and the name of User 2

U2 in association with wireless phone P2 14. An MSID is used to identify the wireless phone during call processing. As indicated above, the MSID used may vary from system to system and additionally at different points within a given system.

Information and parameters defining restrictions or permissive conditions for each supervised user's phone are stored in the User Profile Database 32. The parameters are employed to control the use of the respective wireless phone or to establish conditions that define when alert or warning messages should be provided with respect to the usage of the supervised phone.

Following the association of the applicable identifier(s) with the respective users, the Web-Server 36 steps the Supervisor S1 10 through a configuration sequence for each user having a phone to be supervised through the Supervisory Control System account. During this process, the Web-Server 36 presents the terms and conditions applicable to the service and requests that the Supervisor S1 10 accept the terms and agree to payment of a predetermined monthly fee for each wireless phone that is subject to control of the Supervisory Control System 22.

The Supervisor S1 10 also enters user profile data to be stored within the User Profile Database 32. The user profile data specifies how the respective wireless phone may be used and characteristics associated with such usage. The user profile data may impose restrictions on the use of a phone associated with the user profile data or, alternatively, may specify that warnings and/or alerts regarding phone usage are to be provided to the User or Supervisor S1 10 without restricting phone use. Such warnings or alerts may indicate that usage restrictions are in effect or provide alerts that pertain to the amount of phone usage.

The user profile data described below corresponds to the data that may be entered for a single user. It should be

recognized that the same process is repeated for each user specified by the Supervisor S1 10 within the Supervisory Control System account.

By way of example, and not limitation, the Supervisor S1 10 enters the following information from the access point 42 via a browser interface in response to prompts by the Web-Server 36.

3. Event Control

3a. Overall Usage Limits

The Supervisor S1 10 may optionally specify an overall usage limit for a respective user. The overall usage limit specifies the number of minutes that the wireless phone associated with that user may be used within a predetermined control period, such as a week, a month or any other suitable interval. For example, the predetermined control period may correspond to a weekly or monthly period specified by the Supervisor S1 10, a billing period, or a calendar month, and may be revised from time to time by the Supervisor S1 10 via the Web-Server 36 interface or through a service representative who updates the User Profile Database 32. Once the user of a supervised phone uses a number of minutes equal to the overall usage limit allotted for the control period, no further incoming or outgoing calls are permitted until the next control period, except for calls to or from always-accessible numbers as discussed below. If the usage limit is set to 0 minutes, the phone will only be usable for calls to/from always-accessible numbers that are defined by the Supervisor S1 10. As an exception to the restrictions discussed in the preceding two sentences, in the case of an incoming call that is placed to a restricted phone using a valid cut-through code as described below, the call is connected and in one embodiment, the call

time associated with such a call is not assessed against the user's usage limit.

In one embodiment, the time on calls to or from the always-accessible numbers are not applied against the overall usage limit. For example, it may be desirable for a child to be able to call or be called by a parent without exhaustion of the overall usage limit established by the parent. In such event, the Supervisor (parent) may establish a usage limit and calls made to or from the parent are not applied against the overall usage limit.

3b. Warning Messages and Tones

Even if the Supervisor S1 10 does not establish an overall usage limit for a respective user, the Supervisor S1 10 may optionally enter an indication in the user profile information that warnings or alerts regarding phone usage should be provided to the user or supervisor after one or more usage thresholds are reached. For example, the Supervisor may specify in the User Profile Database 32 that usage alerts are to be provided after a predetermined number of minutes and at subsequent intervals. The Supervisory Control System 22 maintains a value reflective of the cumulative usage of the wireless device within the control period. From time to time the Supervisory Control System 22 determines whether the cumulative usage of the wireless device has reached the interval value specified by the Supervisor at which usage alerts are to be provided. During a call, such usage alert may, for example, be provided to the user in the form of a predetermined tone. Pre-call or post-call audible warning messages to a subscribed user may be injected as an audible script as discussed herein via the VRU 38 or alternatively as text messages via a data bearer service to advise the user of the alert condition.

Additionally, alerts may be generated and forwarded to the Supervisor regarding the usage of the supervised phone at periodic usage intervals. More specifically, the Supervisor may specify a usage interval at which alerts are to be generated and store a value corresponding to the usage interval in the User Profile Database in association with an identifier of the supervised wireless phone. The Supervisory Control System 22 may then determine when the cumulative usage of the wireless device within a control period equals the usage interval specified by the Supervisor or is an integral multiple of the time interval specified by the Supervisor. An alert message may be generated and forwarded to the Supervisor when the cumulative usage of the wireless phone equals the time interval specified by the Supervisor or is an integral multiple of the specified time interval or at any times specified by the Supervisor. The alert may be forwarded to the Supervisor as an audible script, by a text messaging service or alternatively, via email delivery. When forwarding an alert to the Supervisor as an audible script, the message may be communicated to a telephone number specified by the Supervisor and stored in the User Profile Database 32 in association with an identifier for the wireless phone. When forwarding an alert message to the Supervisor as a text message, the text message may be forwarded to the Supervisor at a telephone number specified by the Supervisor and stored in the User Profile Database 32 in association with the wireless phone identifier. When forwarding the alert message to an email address, the message may be forwarded to an email address specified by the Supervisor and stored in the User Profile Database 32 in association with the wireless phone identifier. The alert message may also be communicated to the Supervisory account by the Web Server 36 and accessed by the Supervisor either at the Access Point 42 or via a personal computer, mobile phone, or

personal digital assistant (PDA) having access to the Web Server 36. At the beginning of each control period (e.g. each month) the value maintained by the Supervisory Control System 22 pertaining to the cumulative usage of the wireless phone may be reset to reflect no usage of the wireless phone within the new control period.

The above-described alerts may be forwarded to the Supervisor and/or User with or without the imposition of restrictions on the use of the supervised phone.

3c. Permitted/Non-Permitted Usage Periods

Within the user profile data, the Supervisor S1 10 may specify time periods during which general phone use is permitted or not permitted. Whether an embodiment of the disclosed system provides for the specification of prohibited usage times or permitted usage times is a matter of design choice.

By way of example, and with reference to Fig. 1, within the user profile data, the Supervisor S1 10 may specify that User U1 44, who for purposes of illustration is assumed to be a young child, is not permitted to use the supervised wireless phone P1 12 for general usage calls other than between 4pm and 8pm on weekdays and between 9am and 8pm on weekends and holidays.

If the overall general usage limit for the specified control period is set to 0 minutes for a particular supervised phone, the system permits calls only to and from always accessible numbers and additionally, calls to the supervised phone using a valid cut-through code as discussed below.

3d. Location Controls

Also within the user profile data, the Supervisor S1 10 may specify one or more geographic locations or geographic

areas within which general phone use is permitted or not permitted. Whether an embodiment of the disclosed system provides for the specification of prohibited usage locations or geographic areas, or permitted usage locations or geographic areas, is a matter of design choice. The Supervisor may specify the geographic location as a street address and a converter or conversion service, as known in the art, may be employed to resolve the street address into a set of coordinates in a predetermined coordinate system. For example, the street address specified by the Supervisor may be stored in the User Profile Database 32 and converted into latitude and longitude coordinates prior to use. Following conversion of the street address into coordinates represented within the specified coordinate system, the coordinates may be stored within the User Profile Database so that the conversion need not be performed each time a call to or from the respective wireless device is made.

The location of the phone is generated using a global positioning system, cell sector identifiers or any other suitable technique for generating coordinates defining the location of the phone. More specifically, cell sector identifiers may be employed to resolve the geographic location of the wireless phone. The function of determining the geographic location of a wireless phone is performed via the use of a location server 57, also known as a location service broker. Such services are commercially available. One company that offers location service broker services is Apertio Limited, Kingswood, Bristol, United Kingdom and such services are described at www.invergence.co.uk. More specifically, the location service broker is operative to convert cell sector identifiers into a coordinate system such as latitude and longitude for subsequent use.

Alternatively, location information regarding the current location of the supervised wireless phone P1 12 may be obtained through the use of a GPS (Global Positioning System) receiver disposed within the wireless phone.

After determination of the geographic location of the phone, the location of the wireless phone is compared to the geographic location specified in the User Profile Database 32 to determine if a call should proceed. More specifically, the Supervisor may specify a distance between the location specified in the User Profile Database and the location of the wireless phone within which the location of the wireless phone is deemed to correspond to the location specified by Supervisor. If the location of the wireless phone corresponds to at least one location specified by the Supervisor within the User Profile Database 32, the call may be permitted to be completed or the connection of the call may be prevented based upon the parameters specified by the Supervisor in the User Profile Database 32 in the event of such a correspondence. By way of example, and with reference to Fig. 1, within the user profile data, the Supervisor S1 10 may specify that User U1 44, who for purposes of illustration is assumed to be a young child, is not permitted to use the supervised wireless phone P1 12 for general usage calls when the phone is generally within the geographic area defined by the school grounds of User U1 44.

Any appropriate technique for definition of such a restricted area may be used. For example, an indication of a restricted address, combined with the radius of the area to be considered restricted around that address, may be entered by the Supervisor S1 10 into the user profile data to provide the restricted area definition.

The present system may be embodied to allow the definition of restricted or permitted phone use locations for incoming calls, outgoing calls, or both.

i. Use of Cell Sector Identifiers

The Supervisory Control System 22, in one embodiment, obtains cell sector identifiers and uses the cell sector identifiers alone or in combination with associated signal strength information to obtain the location coordinates of the wireless phone. More specifically, the wireless phone has access to the received radio signal transmission strength at the mobile station radio transceiver (P1, P2). A processor on the wireless phone may execute a script or application that enables the wireless phone to calculate, extract and transmit signal strength measurements to the network via a non-displayable SMS message or via any other suitable protocol. The signal strength data is coupled with the cell sector identifier information and the location area code that may be obtained from the home location register (HLR) 56. The signal strength and cell sector identifier information may then be forwarded to the location server 57 to calculate coordinates of the mobile station. The location server 57 may generate coordinates using the cell sector identifiers alone or in combination with the signal strength information to resolve the wireless phone coordinates with greater accuracy. In particular, the Supervisory Control System 22 communicates the cell sector identifiers and optionally the signal strength information to the commercially available service provider, such as the location server 57, to map cell sector identifiers and signal strength data into coordinates that identify the location of the wireless phone. The location server may also be employed to map street address or address information entered in the Profile Database by the Supervisor into

coordinates that are returned to the Supervisory Control System 22.

It should be recognized that the mapping of street address information to latitude and longitude information may also be performed by the Supervisory Control System 22. In the circumstance in which the mapping is performed by the Supervisory Control System 22, the Supervisory Control System 22 would include the location server 57 functionality.

The Supervisory Control System may include a program that inspects the HLR 56 at specific time intervals, obtains or derives the latitude and longitude of the supervised phone at each such time, and arithmetically derives a speed of the supervised phone based upon the location information and the time interval. A speed threshold may be stored by the Supervisor in the User Profile Database 32. If the speed threshold is exceeded, a program within the Supervisory Control System may take such actions as are specified by the Supervisor. For example, the Supervisory Control System may be programmed to forward to the Supervisor S1 10 an audible message communicated to a telephone number specified by the Supervisor, a text message via a data bearer service (such as SMS messaging), or an email message that includes an alert that the respective supervised phone has been detected as having exceeded the specified speed threshold. Additionally, the Supervisory Control System may be programmed to communicate a notice to the Supervisor S1 10 via the Web Server 36 that is posted in association with the Supervisory account and accessible by the Supervisor. Moreover, the Supervisory Control System 22 may be programmed to prevent further incoming or outgoing calls or to terminate any call in progress at the time of the detection of the excessive speed condition.

In the event of an outgoing call by a supervised phone, the network inspects the HLR and identifies the telephone as

one being managed by the Supervisory Control System 22. This determination may be made based upon the telephone number of the calling party or any other suitable phone identifier. In response to the determination that the phone associated with the respective phone identifier is managed by the Supervisory Control System 22, the network passes call control to the Supervisory Control System 22. The Supervisory Control System 22 looks up the user profile in the User Profile Database 32 for the calling party. Upon ascertaining that there is a location restriction on phone use, the Supervisory Control System 22 sends an inquiry to the HLR to ascertain the location of the calling party. The HLR returns to the Supervisory Control System 22 the cell sector identifier associated with the calling party. In one embodiment the Supervisory Control System 22 obtains coordinates of the wireless phone using the location server 57 and determines whether the coordinates of the wireless phone correspond to the coordinates corresponding to the address entered into the User Profile Database by the Supervisor.

In another embodiment, the Supervisory Control System 22 compares the cell sector identifier associated with the calling party with the locations identified in the User Profile Database 32. More specifically, using a location server, the addresses entered by the Supervisor are mapped into cell sector identifiers. If the cell sector identifier of the calling party's phone corresponds to a restricted cell sector identifer identified in the User Profile Database 32, the Supervisory Control System 22 provides appropriate signaling to the control network to prevent the call from being connected. It should be appreciated that if the cell sector identifier of the calling phone is forwarded to the Supervisory Control System 22 along with the request for service by the Supervisory Control System

22 a subsequent request for the cell sector identifier can be avoided.

When a call is placed to a supervised phone, the network inspects the HLR and identifies the supervised phone as one that is managed by the Supervisory Control System 32. In response to this determination, call control is passed to the Supervisory Control System 22. The Supervisory Control System 22 looks up the user profile in the User Profile Database 32 for the called party. Upon ascertaining that there is a location restriction on phone use, the Supervisory Control System 22 sends an inquiry to the HLR to ascertain the location of the called party. The HLR returns to the Supervisory Control System 22 the cell sector identifier(s) associated with the called party and optionally signal strength information associated with each of the cell sector identifiers as discussed above. The Supervisory Control System 22 then compares the location of the wireless phone to the location specified in the User Profile Database 32. This comparison may involve a comparison of coordinates after resolving the cell sector identifier data into coordinates or alternatively a comparison of cell sector identifiers to determine if the wireless phone is at a location that corresponds to a location specified by the Supervisor in the User Profile Database 32. The Supervisory Control System 22 provides appropriate signaling to the control network to either permit the call to be connected or to prevent the call from being connected based upon the result of the comparison. It should be noted that if the cell sector identifier of the wireless phone is forwarded to the Supervisory Control System 22 along with the request for service by the Supervisory Control System 22 a subsequent request for the cell sector identifier can be avoided.

ii. Use of GPS Coordinates

Alternatively, GPS coordinates may be employed to provide restrictions on phone use for a supervised phone. As discussed above, the Supervisor S1 10 enters into the User Profile Database 32 a physical address or the identification of a location at which the phone use is restricted or permitted, as applicable. The physical address, street address or identification entered into the User Profile Database 32 by the Supervisor S1 10 is converted into coordinates. More specifically, a converter accepts input information in the form entered by the Supervisor and converts such information into coordinates defining the location of the wireless phone. In the instant example, it is assumed that the Supervisor has entered into the User Profile Database 32 an address at which the use of the supervised phone is restricted.

The Supervisory Control System 22 accesses the location server 57 to obtain the geographic coordinates (latitude, longitude description) corresponding to the restricted/permitted use location specified by the Supervisor as an address. The geographic area in which the use of the wireless phone is restricted may be represented by a set of coordinates defining boundaries, as a mathematical description, as a set of coordinates and a radius defining a circular area, or any other suitable way of describing the geographic area within which the phone use is restricted or permitted. While the presently illustrated embodiment utilizes latitude and longitude coordinates to identify the geographic area of interest, any other suitable coordinate system may be employed. The Supervisory Control System 22 stores the coordinates or mathematical description defining the geographic location in which the use of the wireless phone is restricted.

In one embodiment, the location of the wireless phone is deemed to be at the location specified in the User Profile

Database, if the coordinates of the wireless phone are within a specified distance of the coordinates corresponding to an address specified in the User Profile Database 32. The specified distance may be input by the Supervisor S1 10 and stored in the User Profile Database 32 or a default distance may be specified which may be modified by the Supervisor S1 10.

In response to an outgoing call from a managed phone, the HLR associated with the wireless phone identifies the phone as one that is serviced by the Supervisory Control System 22 and passes control to the Supervisory Control System 22. The Supervisory Control System 22 inspects the User Profile Database 32 and identifies the calling phone as one that has one or more restrictions involving locations of use. The Supervisory Control System initiates a network query to obtain GPS coordinates of the handset which are provided by a GPS receiver contained within the wireless phone. The network query may comprise a query of the wireless phone or any other network element having access to the GPS coordinates of the wireless phone. In response to the network query, the GPS coordinates of the supervised phone are returned to the Supervisory Control System 22.

The coordinates of the wireless phone are then compared by the Supervisory Control System 22 to the restricted area as specified within the User Profile Database 32 to determine to the wireless phone coordinates are within a restricted area. If the coordinates of the wireless phone are within the restricted area, the Supervisory Control System 22 prevents the call from being connected.

Additionally, the Supervisory Control System 22 may include a program that permits the wireless phone or the network to be queried to ascertain the physical location of the phone in response to the receipt of a control code such as "*" or any other suitable control code entered on the keypad of the

wireless phone by the supervised user. Alternatively, the Supervisory Control System 22 may initiate a query to ascertain the location of the supervised phone in response to an inquiry initiated by the Supervisor S1 10. Additionally, the Supervisor may initiate a query to ascertain the location of the wireless phone for one of the supervised Users. The request from the Supervisor may be communicated to the Supervisory Control System 22 from the Supervisor's phone, from the Access Point 42 via the Web Server 36 or via any other communication path. Location information responsive to a request initiated either by the supervised user or the Supervisor may be communicated to the Supervisor audibly via a script played by the VRU 38 to the Supervised User's phone, via text messaging or via email. Prior to communication of the location of the wireless phone to the Supervisor S1 10, a conversion of the wireless phone coordinate data to an address may be performed and address information may be conveyed to the Supervisor instead of coordinate data.

In the circumstance of an incoming call to a supervised phone, a determination is made whether the call may be completed as discussed above.

It should be recognized that if the coordinates of the supervised phone are provided along with the request for service by the Supervisory Control System 22, the network query can be avoided.

iii. Combinations of Restrictions or Permissive Use

The location information obtained via a GPS receiver disposed in the wireless phone, or a system that resolves the wireless phone location using cell sector identifiers, may be employed in conjunction with other restrictions and/or permissions to determine whether a call placed to or from the wireless phone should be connected. For example, Boolean

functions of restrictions and/or permissions described herein and the location information may be generated to determine whether a call should be connected or blocked. More specifically, a location restriction may be employed in conjunction with a time period restriction to prevent the wireless phone from being used for normal calls while a child is at school and during the normal school hours of 9am to 3pm. Thus, the child could make and receive calls while at school before and after the normal school day or while away from the school. Similarly, location restrictions may be employed in conjunction with one or more lists of always accessible numbers and/or one or more lists of never accessible numbers to allow or disallow calls to/from specific numbers based upon the location of the supervised wireless phone and the telephone numbers on the lists of always accessible numbers and/or never accessible numbers as applicable. Finally, a determination may be made by the Supervisory Control System 22 whether to complete or block a call based upon a combination of one or more of the wireless phone location, always accessible or never accessible numbers, date, day or the week and/or a permitted or restricted time period.

While the restrictions and/or permissions regarding phone usage are entered by the Supervisor S1 10 into the User Profile Database 32 for the respective wireless phone, information representative of the location information stored in the User Profile Database may be downloaded from the User Profile Database 32 to a first memory region within the wireless phone and a determination may be made within the wireless phone whether to connect a call dialed by the wireless phone user based upon a comparison of the downloaded information to location information generated within the wireless phone. Such a determination may be made using a processor within the wireless phone that executes a software program stored in a

second memory region within the phone. The first and second memory regions may be within the same physical memory or different physical memories within the wireless phone. For example, if a supervisor has entered into the respective User Profile Database 32 a restriction on phone use that indicates that the wireless phone may not be used when a student is at school between 9am and 3pm, a determination may be made by the processor within the wireless phone whether the phone is at the restricted location and whether the current time is within the specified time period, in which event the call may be blocked. By making such a determination within the wireless phone rather than at the Supervisory Control System 22, unnecessary network traffic is avoided. It should be recognized that the location information stored within the User Profile Database 32 may comprise conventional street address information which may be converted to latitude and longitude coordinates prior to communication to the wireless phone. Thus, a comparison of the latitude and longitude coordinates corresponding to the street address entered by the Supervisor 81 10 may be made with respect to the latitude and longitude coordinates obtained from a GPS receiver disposed within the wireless phone and a determination may be made that the wireless phone is at the address specified by the Supervisor if a distance between a location specified by the latitude and longitude associated with the street address and a location specified by the latitude and longitude obtained from a GPS receiver within the wireless phone is less than a predetermined threshold distance. If the wireless phone is determined to be at the address specified in the User Profile Database 32, the call may be terminated or connected as specified by applicable rules maintained within the User Profile Database 32.

3e. Cut-Through Capability

A Supervisor or other individual that desires to call a supervised user's phone (assuming the phone is on and not otherwise in use), may always reach the user's phone provided that a cut-through code has been established for the respective Supervisor or entered by the Supervisor. More specifically, in one embodiment, in response to prompting by the Web-Server 36, the Supervisor S1 10 may provide a cut-through code that is typically defined as being between n and m numerical characters in length. For example a numeric code between 4 and 6 characters in length may be employed. The cut-through code allows the Supervisor S1 10 to access one or more of the supervised phone(s) during hours or under circumstances in which phone usage is restricted and when the Supervisor S1 10 is not located at an always-accessible number. The cut-through code is communicated from the access point 42 to the web server 36 via the communications network 28. The web server communicates the cut-through code over a data path to the User Profile Database 32 for storage. The data path may include a computer that forms a component of the business logic 34 and that writes the cut-through code to the User Profile Database 32.

In one embodiment, as a default, the cut-through code is assigned based upon the Supervisor's user name that is communicated from the access point to the User Profile Database 32. For example if the Supervisor's user name is "abcdef" the cut-through code would be "222333" which represent the number keys on a typical phone keypad that correspond to the letters in the username. If the username were "222333", the cut-through code would be "222333". By way of further example, if the username were "abc444", the cut-through code would be "222444". If the username were more than six characters in length, the cut-through code may be truncated at a

predetermined number of characters, such as at six characters. By using the username as the default cut-through code, the necessity to have the Supervisor input this code is avoided. The Supervisor may be permitted to modify the default cut-through code to specify a different cut-through code to provide higher security.

The Supervisor may also convey the cut-through code to an administrator orally and the administrator may input the cut-through code to the Supervisory Control System 32.

When a Supervisor having knowledge of the cut-through code calls a supervised phone at a time when the use of the phone is subject to a restriction on use, a message is played to the calling party (the Supervisor) that indicates that the called phone is not accessible. If the Supervisor successfully enters the cut-through code before a predetermined time interval expires, the call is allowed to proceed. If the cut-through code is not entered within the predetermined time interval, the call is blocked. If the call is allowed to proceed, a control message of a first type is forwarded to the control network to signal that the call should be connected. If the call is not to be connected, a control message of a second type is forwarded to the control network to prevent the call from being connected.

The "cut-through" capability may be tested during the user profile data setup. At such time, the Supervisor S1 10 may have physical possession of the phones controlled under the Supervisory Control System account before the phones have been distributed to their users. More specifically, in response to prompting from the Web-Server 36, the Supervisor S1 10 powers on the respective user's phone, which is subject to at least one use restriction, and attempts to call it. When the Supervisor S1 10 hears a prompt advising that the phone is not presently reachable, the Supervisor S1 10 enters the previously

selected cut-through code. If the cut-through capability is functioning properly, the respective user's phone rings as a result of the entry of the cut-through code.

3f. Always-Accessible Numbers

In response to a prompt from the Web-Server 36, the Supervisor S1 10 may optionally enter a first list of telephone numbers that may always be called by the respective user and a second list of numbers that may always call the respective user's phone number assuming the wireless phone is powered on and reachable within the wireless network. These lists may be provided as separate lists or alternatively, may be aggregated as a single list. Optionally, the Supervisor S1 10 may enter or associate within the user profile data short codes that correspond to the always-accessible numbers so that one or more of the always-accessible numbers can be rapidly called in an emergency situation without the need for a user to remember the numbers.

3g. Never-Accessible Numbers

In response to a prompt from the Web-Server 36, the Supervisor S1 10 may optionally enter a list comprising one or more telephone numbers or telephone number prefixes that the user of an associated phone should never be able to call and a list of telephone numbers or telephone number prefixes that should never be able to call the supervised user's phone. These lists may be entered as separate lists or alternatively may be aggregated as a single list.

3h. Saving of User Profile Data

When the Supervisor S1 10 initiates the saving of the user profile data, that data is associated with the respective user. If the Supervisor S1 10 exits the setup routine without

saving the user profile data, the respective wireless number is provisioned within the Supervisory Control System 22 for unrestricted use.

3i. Setup of Additional Users

The Web-Server 36 may prompt the Supervisor S1 10 to determine whether he/she desires to utilize the same user profile data for the next user that needs to be configured. The Supervisor S1 10 may apply the previously entered user profile data for the setup or the next user or alternatively, establish a new user profile for the next user. Moreover, as further discussed below, user profiles may be defined and modified on a user group basis. Under such circumstances, the disclosed system enables the Supervisor S1 10 to define a set of user profile parameters that apply to a group of phones and associated users. The control parameters for the group can subsequently be modified and members of the group added or deleted.

4. Supervisory Control System Operation

4a. Supervisory Control System Operation for Incoming Calls to a User

Operation and signaling for the Supervisory Control System 22 with respect to a telephone call that is placed to a user is described below with respect to the devices in Fig. 1 and the steps shown in Fig. 3.

The following example describes an exemplary call from a calling party U5 52 from a telephone P5 50 to a called party U2 46 at a supervised wireless phone P2 14. It is assumed for purposes of the present discussion that Supervisor S1 10 established a user profile applicable to phone P2 14 at a prior time and that the user profile for the phone P2 14 prohibits

general phone usage during school hours from 8:00am to 4:00pm weekdays.

The call placed by caller U5 52 from phone P5 50 is received at an associated Signal Switching Point (SSP 2) 54 as depicted at step 80 of Fig. 3. The Signal Switching Point (SSP 2) 54 accesses the Dialed Number Identification Service (DNIS) which includes the dialed telephone number for the call. From the DNIS, the SSP identifies the service provider for the dialed phone number and routes the call to the applicable service provider. In the instant example, the call is routed to SSP 1 20 which is within the home serving system for the wireless phone P2 14.

The SSP 1 20 within the home serving system for the called number extracts a MSID from the DNIS. The SSP 1 20 performs a lookup within the Home Location Register (HLR) 56 using the extracted identifier to obtain the HLR record for the respective called wireless phone P2. The HLR record includes data that instructs the respective Signal Switching Point (SSP 1) 20 what to do next. If the HLR record indicates that the Supervisory Control System 22 should be accessed in the event of calls to the respective called party, the Supervisory Control System 22 is signaled. If the HLR 56 does not indicate that the Supervisory Control System 22 should be accessed, the call is connected subject to any other restrictions and protocols that may be applicable.

In the instant example, the HLR record includes information that instructs the SSP 1 to signal the Supervisory Control System 22 that an incoming call is pending. More specifically, as depicted at step 82 of Fig. 3, the respective SSP (SSP 1) 20 signals the SCP 24 within the Supervisory Control System 22 that an incoming call is pending for a called party having a specified MSID. The Service Data Point (SDP) 30 within the Supervisory Control System 22 performs a lookup

within the User Profile Database 32 as depicted at step 84 of Fig. 3 to ascertain whether the MSID corresponds to a user profile within the User Profile Database. If as a consequence of the lookup, it is determined that the MSID corresponds to an MSID within the User Profile Database 32, the Business Logic 34 executes a software program as shown at step 86 of Fig. 3 to determine how the call should be handled. As a result of the Business Logic 34 processing, the SCP 24 may be instructed to initiate SS7 signaling and a VRU such as VRU 38 may be instructed to play an audible script to a supervised phone or a calling party. More specifically, if the MSID of the called party corresponds to the MSID of a phone within the User Profile Database 32, the Business Logic 34 within the SDP 30 accesses the relevant data within the applicable records of the User Profile Database 32, current conditions, such as time, date, calling number, and called number and determines what action should be taken. Exemplary Supervisory Control System processing under the control of the Business Logic 34 is described below with reference to Fig. 4.

As depicted at step 90 of Fig. 4, the Business Logic 34 determines at step 90 of Fig. 4 whether the calling number corresponds to an always-accessible telephone number that can always be put through to the supervised phone P2 14. If the calling number corresponds to a telephone number that is specified in the User Profile Database 32 as being an always-accessible number that can always access phone P2 14, the SCP 24 within the Supervisory Control System 22 signals the SSP 1 20 associated with the phone P2 14 (in the instant example SSP 1 20) to allow the call to be connected to the phone P2 14 as indicated at step 92. In response, the call is routed through the MSC 18 in SSP 1 20 to P2 14 to establish the desired connection between P5 52 and the supervised wireless phone P2 14.

If the Business Logic 34 determines, as depicted at step 90, that the calling number does not correspond to a number that can always access the respective phone P2 14, the Business Logic 34 next determines whether the calling number corresponds to a number that is identified within the User Profile Database 32 as never being permitted to access the phone P2 14 as depicted at step 93 of Fig. 4. If the Business Logic 34 determines that the calling number is on the list of never-accessible numbers as depicted at step 93, the Business Logic 34, in conjunction with the SCP 24 may cause a connection in the form of a T1 link or any other suitable communication link to be established between the Intelligent Peripheral or Voice Response Unit (VRU) 38 and the MSC 18. The MSC 18 then couples the VRU 38 through to the calling party. An audible message specified by the Business Logic 34 is played to the calling party by the VRU 38 to indicate that the called party is not accessible as depicted at step 94. The SCP 24 then causes the T1 connection between the VRU 38 and the MSC 18 to be torn down and the SCP 24 signals the Signal Switching Point SSP 1 20 to disconnect the call from the calling party.

If the Business Logic 34 determines that the number of the calling party does not correspond to an always-accessible number or a never-accessible number, as depicted at step 96, the Business Logic determines whether the present time is within a period during which general phone usage is prohibited, e.g. between 8:00am and 4:00pm on a weekday in the instant example. If the present time is within a prohibited period, the Business Logic 34 causes a connection to be established between the VRU 38 and the calling phone P5 50 and causes the VRU 38 to play a message indicating that the called phone is not accessible at the present time as shown at step 97 of Fig. 4. If a cut-through code is entered within a predetermined time period as depicted in step 98, the Business Logic 34

verifies the cut-through code and the SCP 24 signals the MSC 18 to connect the calling party to the supervised phone P2 14 as shown in step 102 by forwarding a control message of a first type. If the proper cut-through code is not entered within the predetermined time period, the Business Logic 34 causes the SCP 24 to initiate SS7 signaling via a control message of a second type that causes the T1 connection between the VRU 38 and the MSC 18 to be broken and the call to be released as depicted in step 104.

If the Business Logic 34 determines that the present time is not within a time period specified within the respective user profile as a period during which general phone usage is prohibited per step 96, the Business Logic 34 determines whether a limit has been established for the number of minutes the phone may be used within a control period and whether the number of allotted minutes for the applicable control period have been exhausted as depicted at step 100. If the total number of allocated minutes for the control period have been exhausted, the Business Logic 34 in conjunction with the SCP 24 causes a connection to be made between the VRU 38 and the calling party via the MSC 18, and causes a message to be played by the VRU 38 indicating that the called party is not accessible as shown at step 97 of Fig. 4. If a proper cut-through code is entered within a specified time period, the Business Logic 34 causes a control message of a first type to be forwarded to the MSC 18 to signal the MSC 18 that the call should be connected. If the predetermined time period has expired without entry of a proper cut-through code, the Business Logic 34, in conjunction with the SCP 24, causes the connection between the VRU 38 and the MSC 18 to be torn down. The Business Logic 34 also initiates signaling of the MSC 18 via a control message of a second type that indicates that the call should not be completed.

If the Business Logic 34 determines that the allocated minutes for the control period for the called party have not been exhausted, the Business Logic 34 next determines whether the calling party has called the supervised user's phone when the phone happens to be at a geographic location at which the use of the phone is restricted as depicted in step 106. If it is determined in step 106 that the called phone is not at a location at which the use of the phone is restricted, the Business Logic 34 initiates signaling of the MSC 18 to cause the call from the calling party to the supervised user's phone P2 to be connected as depicted at step 108.

If the incoming call is placed to the supervised phone at a time when the supervised phone is at a location at which the use of the phone is restricted, a message may be played to the calling party advising that the called phone is not accessible as discussed above with respect to step 97. If a proper cut-through code is not entered within the predetermined time period, the Business Logic 34 initiates signaling of the MSC 18 to prevent the call from being connected as shown in step 104. Alternatively, if the calling party enters the applicable cut-through code as depicted in step 98, the Business Logic initiates signaling of the MSC 18 to instruct the MSC 18 to connect the call as shown in step 102.

It should be recognized that the order of the above steps may be varied and/or selected types of restrictions may be omitted, without departing from the presently disclosed invention and that the present invention involves the functions that are provided rather than the particular order in which such functions are realized. Additionally, the tests applied by the Business Logic 34 may be tests framed in the context of permissive use of the supervised phone rather than in terms of restrictions on use of the supervised phone. By way of example, the User Profile Database 32 in one embodiment includes

parameters that define time intervals during which calls are permitted and/or locations at which calls are permitted. The Business Logic 34 in such embodiment is operative to test the current time to determine if the current time is within a time period during which use of the phone is permitted and/or test the current location to determine if the phone is at a location at which use of the phone is permitted. The Business Logic 34 initiates appropriate signaling to the MSC 18 depending upon the outcome of the comparisons.

Appropriate signaling between the MSC 18 and the Business Logic 34 via the SCP 24 is maintained to update the call usage information so that the number of minutes used by the supervised user within the respective control period does not exceed the total number of minutes allotted for general phone usage within the control period. Thus, the SCP 24, in response to a command from the Business Logic 34 may signal the home serving system MSC 18 to release a call upon a determination that the total minute allotment for the control period has been exhausted or allow the respective call to complete as discussed below. Prior to causing a call to be released due to the exhaustion of the total allotted minutes within the applicable control period, the Supervisory Control System 22 may cause a tone to be injected into the ongoing call between the calling party and the supervised phone to indicate to the respective subscribed user that the call is to be released after a predetermined period. This function may be initiated by the SCP 24, the Business Logic 34, or a combination of both depending upon the design partitioning in a given system. The warning tone may be played by the VRU 38 or injected via any other suitable device.

In an alternative embodiment, even if the total number of minutes used by a supervised user within a control period is exceeded during the pendency of a call, the Supervisory Control

System 22 permits the call to continue to its completion by the parties. Subsequent general usage calls are blocked until a new control period commences or until modification of the usage controls within the User Profile Database 32 by the Supervisor S1 10 so as to permit further general usage calls.

4b. Supervisory Control System Operation for Outgoing Calls from a Supervisory Control System Subscriber

Operation and signaling of the Supervisory Control System 22 with respect to an outgoing telephone call that is placed by a Supervisory Control System 22 subscriber P2 14 is described below with respect to Fig. 1 and flow charts of Fig. 5 and 6. Fig. 1 is employed to illustrate the circumstance in which the wireless supervised phone P2 14 places a call to phone P5 50 that is initially received by the MSC 18 of the home serving system. It is assumed for purposes of the present discussion that Supervisor S1 10 has established a user profile for phone P2 14 and that the user profile for the phone P2 14 prohibits general phone usage during school hours from 8:00am to 4:00pm weekdays.

In the instant example, the call is placed by a calling party U2 46 from wireless phone P2 14 to a called party and is received at step 110 of Fig. 5 by the associated MSC 18 in SSP 1 20 as shown. The MSC 18 associated with SSP 1 20 accesses the respective Home Location Register (HLR) 56 and performs a lookup based on an extracted MSID. The HLR 56 contains a record that includes an indication whether service is required by the Supervisory Control System service provider. If an entry in the applicable HLR record indicates that the Supervisory Control System 22 should be signaled to advise of the pending call, SSP 1 20 signals the SCP 24 within the Supervisory Control System 22 to indicate that there is a pending call as depicted at step 112. If the applicable HLR record does not indicate that

Supervisory Control System services are required, the call is processed in accordance with conventional call processing protocols.

Once the Supervisory Control System 22 receives a signal indicating that a call is pending from a Supervisory Control System subscriber, the Business Logic 34 within the SDP 30 of the Supervisory Control System 22 executes a program to determine what services and signaling need to be initiated by the Supervisory Control System 22.

More specifically, as depicted at step 114 of Fig. 5, the Business Logic 34 performs a lookup within the User Profile Database 32 to ascertain whether the MSID of the calling party corresponds to an MSID within the User Profile Database 32. If, as a consequence of the lookup, it is determined that the MSID corresponds to an MSID within the User Profile Database 32, the Business Logic 34 executes a program to ascertain how the call should be handled. In particular, if the MSID of the calling party corresponds to the MSID of a phone having a record within the User Profile Database 34, the Business Logic 34 accessees the relevant data within the applicable record of the User Profile Database 32, accesses current state information, such as time, date and calling number, and determines what action should be taken as illustrated at step 116. An exemplary series of steps that may be executed within the Business Logic 34 is described below with reference to Fig. 6.

As shown at step 120 of Fig. 6, the Business Logic 34 determines whether the called number corresponds to an always-accessible telephone number, i.e. a telephone number that can always be accessed by the respective phone P2 14. For example, in the instant example, it is assumed that calls to one or more numbers associated with the Supervisor S1 10 (such as the Supervisor's home and wireless numbers) may always be

completed. If the called number corresponds to a telephone number that is specified in the User Profile Database 32 as being always accessible, the Business Logic 34 signals the SCP 24 that the call can be put through as depicted at step 122, and the SCP 24 signals the MSC 18 then associated with the phone P2 14 to allow the call to be connected to the called party. In response, the SSP 1 20 routes the call from phone P2 14 through to the called party to establish the desired connection.

If the Business Logic 34 determines that the called number does not correspond to a number that is always accessible by the phone P2 14, the Business Logic 34 determines whether the called number corresponds to a number that is never permitted to be accessed by the phone P2 14 as illustrated at step 124. This determination is made by obtaining the called number from the DNIS or any other suitable identifier and by comparing the called number to the never-accessible numbers previously entered into the User Profile Database 32 by the Supervisor S1 10. If the Business Logic 34 determines that the called number is on the never-accessible list, the Business Logic 34 may cause a connection to be established between the Intelligent Peripheral or Voice Response Unit (VRU) 38 and the MSC 18 serving the phone P2 14 via a T1 link 60 as shown or via any other suitable communications link. The Business Logic 34 then causes an audible message to be played to the phone P2 14 via the VRU 38 to indicate to the User U2 46 that the called party is not accessible as illustrated at step 126. The Business Logic 34 finally causes the T1 link (or other connection) between the VRU 38 and MSC 18 serving the phone P2 14 to be torn down and causes the SCP 24 to signal the SSP 1 20 to prevent the call from the phone P2 14 to the called number from being connected by forwarding a control message to the SSP 1 20.

If the Business Logic 34 determines that the number of the called party does not correspond to an always-accessible number or a never-accessible number, the Business Logic 34 determines whether the present time is within a period during which general phone usage is prohibited as depicted at step 128, e.g. between 8:00am and 4:00pm on a weekday in the instant example. If the present time is within a prohibited period, the Business Logic 34 causes a connection to be established between the VRU 38 and the MSC 18 associated with the calling phone P2 14 and causes the VRU 38 to play a message indicating that the call cannot be connected at the present time. The Business Logic 34 then causes the T1 link 60 between the VRU 38 and the respective SSP 1 20 to be torn down and causes SCP 24 to signal the MSC 18 by forwarding a control message that indicates that the call should be released as shown at step 126.

If the Business Logic 34 determines that the present time is not within a time period specified within the respective user profile as a period during which general phone usage is prohibited, the Business Logic 34 determines whether the total number of allotted minutes for the month have already been exhausted as depicted at step 130. If the total number of minutes have been exhausted, the Business Logic 34 causes a connection to be made between the VRU 38 and the MSC 18 serving the calling phone P2 14, and causes a message to be played by the VRU 38 to the phone P2 14 indicating that the called party is not accessible as illustrated at step 126. The Business Logic 34 then causes the connection between the VRU 38 and the respective MSC 18 to be torn down and initiates signaling by the SCP 24 to have the call from wireless phone P2 14 released by the serving MSC 18.

If the Business Logic 34 determines that the allotment of minutes for the relevant control period have not been

exhausted, the Business Logic 34 determines if the calling phone P2 is subject to a location restriction as depicted at step 132 and as specified in the User Profile Database 32. If the supervised user's phone P2 14 is subject to a location restriction, the Business Logic 34 causes a connection to be made between the VRU 38 and the MSC 18 serving the calling phone P2 14, and causes a message to be played by the VRU 38 to the phone P2 14 indicating that the called party is not accessible as illustrated at step 126. The Business Logic 34 then causes the connection between the VRU 38 and the respective MSC 18 to be torn down and initiates signaling by the SCP 24 to have the call from wireless phone P2 14 released by the serving MSC 18.

If the Business Logic 34 determines in step 132 that no location restriction is applicable to the use of the phone P2 14, the Business Logic 34 initiates signaling by the SCP 24 to the respective SSP 1 20 to connect the subscriber's phone P2 14 to the called party as shown at step 134.

It should be recognized that the order of the above steps may be varied and/or selected types of restrictions may be omitted.

4c. Updating of Phone Usage Information

Appropriate signaling between the respective SSP 1 20 and the Supervisory Control System 22 is maintained during a call to update the call usage information so that the total allotment of minutes for general phone usage within the control period is not exceeded unless permitted as specified in the User Profile Database 32. Time monitoring may be performed by the SCP 24, the Business Logic 34, or a combination of both based upon the particular design partitioning for the Supervisory Control System 22. Such time monitoring of call length may be performed by the Supervisory Control System 22

via a signaling path between the SCP 24 and the respective MSC 18 that is maintained while the call is pending. The Supervisory Control System 22 updates the minutes remaining and may cause the SCP 24 to signal the SSP 1 20 associated with the calling party to release the call upon determining that the allotment of minutes for the control period has been exhausted if so specified by the Supervisory Control System 22.

In an alternative embodiment, even if the total number of minutes used by a supervised user within a control period is exceeded during the pendancy of a call, the Supervisory Control System 22 permits the call to continue to its completion by the parties. Subsequent general usage calls are blocked until a new control period or modification by the Supervisor S1 10 of the usage controls within the User Profile Database 32 so as to permit further general usage calls.

Other desired supervisory functions may be performed by the Business Logic 34. Signaling between the Supervisory Control System platform 22 and the applicable SSP 1 20 may be accomplished via any suitable signaling technique.

4d. Roaming Scenarios

Fig. 2 depicts the circumstance in which a supervised wireless phone is served by an MSC outside the home system. In the instance in which the subscriber U2 46 is roaming, when the subscriber activates the phone P2 14, the MSC 66 accesses a central database 64 using an MSID for the roaming phone to perform a record lookup. The record retrieved from the central database 64 is used to populate the Visitor Location Register (VLR) 65 for the respective MSC 66 as is known in the art. When a call that is placed from the wireless phone P2 is received by the local MSC 66, the MSC 66 uses an MSID associated with the calling wireless phone P2 to perform a lookup within the VLR 65. The record obtained from the VLR

includes information instructing the MSC 66 to signal the Supervisory Control System 22 if Supervisory Control System services may be required. Once the SCP 24 within the Supervisory Control System is signaled that Supervisory Control System services are required, processing within the Supervisory Control System 22 proceeds generally as described above, noting that appropriate SS7 signaling is employed as is known in the art for completion, release, and VRU messaging of wireless calls initiated from serving systems other than the home serving system.

Additionally, the Supervisory Control System 22 is invoked with respect to calls received by the supervised phone P2 14 when the phone P2 14 is roaming, noting that appropriate SS7 signaling is employed as is known in the art for completion, release, VRU messaging and tone injection for wireless calls that are received by the supervised phone P2 14.

4e. Enterprise Embodiment

While the preceding examples have described operation of the disclosed system in the context of a parent supervising the wireless phones of children, the disclosed system may similarly be used by a manager within an enterprise to control the usage of wireless phones by employees under his or her supervision. For example, a business organization with a number of employees may be broken down as the following example indicates:

Senior Management - 4

Sales - 5

Client and Field Support - 10

In the present example, 19 phones are available for senior management, sales, and client and field support, collectively, and each employee is to be separately allocated a number of minutes for phone use during the control period. The business does not plan to control usage among Senior Management

and Sales employees, but desires to control usage among client and field support employees. Accordingly, the Supervisory Control System account for the business is configured by the responsible manager and the 10 phones provided to the Client and Field Support employees may be treated as a single group of users as further discussed.

The manager navigates to a predetermined Web-site and is prompted to create the necessary Supervisory Control System account. The manager provides his name, company name, service account number for the business, and email address, and creates a login name and password. The manager then defines the wireless phones that are to be controlled under the Supervisory Control System account. The wireless phones under supervision are thus associated with a corporate Supervisory Control System account number for the business. For example, in the case where 10 phones are identified in association with the Supervisory Control System account, an account summary screen may be presented on which an identification of the 10 phones is entered. The manager is then permitted to provision a name next to each of the 10 phones. In one embodiment, by default, the 10 phones are initially setup in a single generic "group" in which they are enabled minimally to call each other. However, though they are initially provisioned to call each other, the manager may further add other names and numbers that the phones should be always available, with respect to calls from and/or to the phones in the initial group, including headquarters numbers, other wireless numbers for employees, etc. Additionally, the manager may establish a specific number of allocated "general purpose" minutes that each phone in the group is allocated to use on a periodic basis. This allocation allows the employee to place calls to other numbers until the allocation has been exhausted. Similarly, a never-accessible list of numbers may be defined for the group. The never-

accessible list includes numbers that cannot be the source or destination number for calls involving the respective supervised phone.

At this point, the provisioning process is complete, and the phones are available for use. The manager, for example, is shown an account summary screen, showing the phones as members of a "Default Group". At a subsequent point in time, the manager may wish to perform management functions with respect to the previously defined Supervisory Control System account. When the manager subsequently logs into the system via the Web server, he or she is again taken to the account summary screen. On the account summary screen, the last view of the managed groups is displayed. For example, an "open" default group folder would be displayed, and a "modify properties" button shown with the 10 phones below it, and showing the MSID, Name, Used/Allocated minutes and a "modify properties" button for each phone. If the manager clicks on the "modify properties" button on for the default group, he or she is enabled to perform the following functions:

(a) Modify the numbers listed under the always-accessible and never-accessible lists, by editing numbers on the lists, and adding or deleting number to or from the lists respectively,

(b) Modify the allocation of minutes for the control period for the group,

(c) Modify any incoming or outgoing call time restrictions associated with the group, and

(d) Modify any other restrictions maintained in the User Profile Database 32 that may be specified by the Supervisor.

When modifying group properties, the modifications take effect for all members of the group. Additionally, the usage properties of the phones may be separately modified. Additionally, where particular messages are specified to be

played on the occurrence of certain associated events, such as call blocking, those messages may be defined on a group wide basis. When it is desired to add new phones to the account, for example, when more phones are purchased for new client services employees, the manager can add those phones to the existing group through the Web Server interface after their service is provisioned by the wireless carrier. When the manager logs onto the graphical user interface provided by the Web server 36, the new phones automatically appear as part of the default group, and automatically take on the properties of the default unless the manager "moves" them, for example by a drag-and-drop operation, into another group. The manager is also enabled to define and/or define the name(s) associated with the new phones through the Web Server 36. In this way, multiple user groups can be defined and named with associated use parameters, and users can conveniently be added to and/or moved between the various groups within an Supervisory Control System account.

Additionally, wireless phones of supervised users may include a resident program that permits a client application to be downloaded from the Supervisory Control System 22. For example a Binary Runtime Environment for Wireless (BREW) application that provides a user interface for quick access to the always-accessible numbers they can call, by name, may be downloaded from the Supervisory Control System 22. Such a client application may be configured to connect to the Supervisory Control System 22 at startup to retrieve always-accessible numbers.

4f. SIM Embodiment

The disclosed system may employ a Subscriber Identity Module (SIM) module within the wireless phone to provide certain filters for outgoing calls from the respective wireless

phone under supervision. In such an embodiment, parameters relevant to outgoing call restrictions may be downloaded or otherwise communicated to the SIM within the respective wireless phone from the User Profile Database 32 and may then be stored on and processed using the SIM when an outgoing call is dialed from the respective wireless phone. By way of example, and not limitation, location restrictions, never-accessible number restrictions, time of day restrictions and/or date restrictions specific to the user may be stored within the SIM of the respective wireless phone. In response to the dialing of an outgoing number, the restrictions applicable to the respective phone and stored within the SIM may be tested to determine whether the connection of the call would be contrary to any restrictions. The processing logic associated with this determination may be made by a processor within the SIM or within the wireless phone. Additionally, the parameters defining the use restrictions (or permissive uses) may be stored on a memory within the SIM or alternatively within portions of a memory shared with program code executed by a processor within the wireless handset. By filtering outgoing calls in the above-described manner, network traffic and external processing is reduced since signaling to the Supervisory Control System 22 is avoided and processing pertaining to calls filtered by the SIM need not be performed by the Supervisory Control System 22. The relevant parameters for such outgoing call restrictions may be updated when the phone is powered on and registered within the wireless network to assure that the parameters reflect the current parameters pertaining to use restrictions for the respective wireless phone.

5. System Architecture

The presently described supervisory system may be employed in conjunction with a billing process for wireless phones. For example, call rating data and other parameters applicable to billing functions may be stored in a first database that is used by a first server to perform the billing functions as known in the art, such as a prepaid billing process for wireless phones.

A second database may be used to store parameters applicable to the presently disclosed supervisory restrictions and a second server executing the presently disclosed supervisory process and including the functions of the Business Logic 34 may be employed to determine whether to connect a call in view of the stored supervisory restrictions.

The supervisory process may operate as an overlay to the billing process. For example, in a prepaid wireless environment, a determination may be made whether sufficient funds have been prepaid for the call to be connected upon execution of the billing process in the first server. If sufficient funds exist in the prepaid account for a call to be connected, the supervisory process may then be executed to determine whether the call should be connected. It should be understood that the order of execution of the billing process and the supervisory process may be reversed. The billing process and the supervisory process may be executed within first and second servers that are separate servers. Alternatively, the first and second servers may comprise the same server and the billing process and the supervisory process may be executed within the same server.

It will be further appreciated by those skilled in the art that while the exemplary embodiments are illustrated in terms of wireless phone communications, the inventive concepts described herein are equally applicable to data messaging services, such as short messaging service (SMS) and the presently disclosed concepts may be employed to restrict or permit such communications. With respect to restrictions on data messaging devices, in addition to restrictions applicable to data communication devices, such as time of day, location, and devices associated with specific individuals, restrictions may be imposed on the number of bytes and/or messages to be communicated during a control period. The determination whether to permit a data communication to be completed may be made at the Supervisory Control System 22. Additionally, determinations whether to restrict outgoing messaging from a wireless device may be made using a processor within the wireless device to reduce network traffic.

Those skilled in the art should readily appreciate that programs defining the functions of the present invention can be delivered to a computer in many forms; including, but not limited to: (a) information permanently stored on non-writable storage media (e.g. read only memory devices within a computer such as ROM or CD-ROM disks readable by a computer I/O attachment); or (b) information alterably stored on writable storage media (e.g. floppy disks and hard drives). In addition, while the invention may be embodied in computer software, the functions necessary to implement the invention may alternatively be embodied in part or in whole using hardware components such as Application Specific Integrated Circuits or other hardware, or some combination of hardware components and software.

While the invention is described through the above exemplary embodiments, it will be understood by those of

ordinary skill in the art that modification to and variation of the illustrated embodiments may be made without departing from the inventive concepts herein disclosed. Accordingly, the invention should not be viewed as limited except by the scope and spirit of the appended claims.

CLAIMS

What is claimed is:

1. A method of controlling the usage of a wireless device comprising the steps of:

obtaining a first set of coordinates in a specified coordinate system representative of a first geographic location;

in response to an attempt to establish a communication involving said wireless device and another communication device:

obtaining a second set of coordinates in said specified coordinate system representative of a second geographic location corresponding to the geographic location of said wireless device;

determining based upon said first and second sets of coordinates, whether said wireless device is at a location where use of said wireless device is restricted; and

based on the result of said determining step, if said wireless device is at a location where use of the device is restricted, preventing said attempted communication involving said wireless device and said other communication device.

2. The method of claim 1 further including the step of permitting said attempted communication if said wireless device is not at a location where use of said wireless device is restricted.

3. The method of claim 2 wherein said preventing step includes the step of generating a control message of a first type and said permitting step includes the step of generating a

control message of a second type and forwarding one of said control messages of said first and second types to signal whether said attempted communication should be prevented or permitted.

4. The method of claim 3 wherein said determining step comprises the step of determining a first distance between said second geographic location specified by said second set of coordinates and said first geographic location specified by said first set of coordinates and said control message generating steps comprise the steps of generating said control message of said first type in the event said first distance is greater than a specified threshold and generating said control message of said second type in the event said first distance is less than said threshold distance.

5. The method of claim 1 wherein said wireless device is a wireless phone, said other communication device is another phone and said attempted communication is an attempted call involving said wireless phone and said other phone.

6. The method of claim 1 wherein said wireless device is operative to communicate via a data messaging protocol and said other communication device is operative to communicate via said data messaging protocol.

7. The method of claim 1 further including the steps of:

receiving as an input at an access point information corresponding to said first geographic location;

communicating said information corresponding to said first geographic location over a first communication network to a first server communicably coupled to a database for storage in said database; and

storing said first geographic location in said database.

8. The method of claim 7 further including the steps of:

receiving at said access point a password input by a user;

communicating said password from said access point over said first communication network to said first server;

comparing said password input to said access point to a stored password associated with a supervisory account; and

performing said storing step in the event said password input at said access point corresponds to said stored password.

9. The method of claim 8 further including the steps of:

associating at least one user account with said supervisory account, wherein each of said at least one user account is associated with a corresponding wireless device; and

storing in said database said information corresponding to said first geographic location in association with said one of said at least one user account.

10. The method of claim 9 wherein said associating step comprises the step of associating a plurality of user accounts with said supervisory account; and

said storing step comprises the step of storing in said database said information corresponding to said first geographic location in association with one of said plurality of user accounts.

11. The method of claim 1 wherein said step of obtaining said first set of coordinates includes the steps of:

storing in a database a location identifier associated with said first geographic location; and

converting said location identifier corresponding to said first geographic location into said first set of coordinates in said specified coordinate system and storing said first set of coordinates in said database.

12. The method of claim 11 wherein said location identifier comprises an address and said storing step comprises the step of storing said address in said database

13. The method of claim 11 wherein said database is communicably coupled to a first server and said converting step comprises the steps of:

retrieving said location identifier from said database;

forwarding said location identifier to a location server;

converting said location identifier into said first said of coordinates at said location server; and

forwarding said first set of coordinates to said first server for storage in said database.

14. The method of claim 1 further including the steps of:

storing in a database a time specification,

utilizing said time specification and location information corresponding to said first geographic location to determine whether to permit said attempted communication involving said wireless device and said other communication device.

15. The method of claim 14 wherein said time specification comprises a time period and said utilizing step comprises the step of determining whether a current time is within said time period.

16. The method of claim 14 wherein said time specification comprises at least one day of the week and said utilizing step comprises the step of determining whether a current day of the week matches said at least one day of the week.

17. The method of claim 14 wherein said time specification includes at least one date specification and said utilizing step comprises the step of determining whether a current date matches said at least one date specification.

18. The method of claim 1 further including the step of:

forwarding said control message to an external device; and

determining at said external device, based on said control message, whether said attempted communication should be completed or terminated.

19. The method of claim 1 wherein said step of obtaining said second set of coordinates in said specified coordinate system comprises the step of obtaining said second set of coordinates from a global positioning system receiver disposed in said wireless device.

20. The method of claim 19 further including the steps of:

communicating said first set of coordinates to said wireless device and retrievably storing said first set of coordinates in a memory in said wireless device, wherein said memory is in communication with a processor within said wireless device; and

responsive to the initiation of a communication from said wireless device to said other communication device:

retrieving said first set of coordinates from said memory using said processor within said wireless device;

performing said determining step within said processor utilizing said retrieved first set of coordinates and said second set of coordinates obtained from said global positioning system receiver; and

responsive to said performing of said distance determining step by said processor within said wireless phone, determining in said processor whether to prevent said communication from said wireless device to said other communication device.

21. The method of claim 1 further including the steps of:

responsive to said attempted communication involving said wireless device and said other communication device by one of said wireless phone and said communication device:

retrieving at least one cell sector identifier associated with the geographic location of said wireless phone;

forwarding said at least one cell sector identifier to a location server; and

generating said second set of coordinates within said location server based upon said retrieved at least one cell sector identifier.

22. The method of claim 21 wherein said cell sector identifier retrieving step further includes the step of retrieving a signal strength that is associated with each of said at least one cell sector identifier, wherein said forwarding step includes the step of forwarding said signal strength associated with each of said at least one cell sector identifier to said location server with the respective cell sector identifier; and

said second set of coordinates generating step comprises the step of generating said second set of coordinates from said

at least one cell sector identifier and the signal strength associated with each of said at least cell sector identifier.

23. A system of controlling the usage of a wireless device comprising:

a storage device containing a user profile database, said user profile database storing a first set of coordinates representative of a first geographic location;

at least one first processor in communication with said user profile database, said at least first processor operative in response to an attempt to establish a communication involving said wireless device and another communication device:

to obtain a second set of coordinates representative of a second geographic location corresponding to a geographic location of said wireless phone;

to determine based upon said first and second set of coordinates whether said wireless device is at a location at which use of the wireless device is restricted;

to generate a control message of a first type in the event said determining step indicates that said wireless device is at a location at which the use of the wireless device is restricted; and

to generate a control message of a second type in the event said determining step indicates that said wireless device is at a location at which the use of the wireless device is not restricted and to utilize said distance in the determination whether the use of said wireless device is restricted.

24. The system of claim 23 wherein said at least one first processor is operative to determine a distance between said second geographic location specified by said second set of

coordinates and said first geographic location specified by said first set of coordinates and to generate said control message of said first type in the event said distance is less than a specified distance value and to generate said control message of said second type if said distance is greater than said specified distance value.

25. The system of claim 23 further including a wireless device having a global positioning system receiver disposed therein, said global positioning system operative to generate said second set of coordinates representative of the geographic location of said wireless phone.

26. The system of claim 25 wherein said wireless device includes logic operative to forward said second set of coordinates to said at least one first processor for use in the determination of whether the wireless device is at a location at which the use of the wireless device is restricted.

27. The system of claim 23 wherein said user profile database further includes a location identifier associated with said first geographic location, said system further including a converter operative to generate said first set of coordinates from said location identifier.

28. The system of claim 27 wherein said location identifier comprises an address.

29. The system of claim 27 wherein said converter comprises a location server.

30. The system of claim 23 wherein said at least one first processor in communication with said user profile database is

operative to calculate a distance between said first and second geographic locations using said first and second sets of coordinates and to generate a message indicating that said attempted communication should be prevented in the event the distance between the first and second geographic locations is less than a predetermined threshold distance.

31. The system of claim 23 wherein said at least one first processor in communication with said user profile database is operative:

to retrieve at least one cell sector identifier indicative of the location of said wireless device;

to forward said at least one cell sector identifier to a location server; and

to receive from said location server said second set of coordinates.

32. The system of claim 31 wherein said at least one first processor in communication with said user profile database is further operative:

to retrieve at least one signal strength value associated with at least some of said cell sector identifiers;

to forward to said location server, said at least one cell sector identifier and the associated signal strength value; and

to receive from said location server said second set of coordinates derived from said at least one cell sector identifier and the associated signal strength value.

33. A system of controlling the usage of a wireless device comprising:

a supervisory control system comprising:

a storage device containing a user profile database, said user profile database storing a first set of coordinates in a specified coordinate system representative of a first geographic location; and

at least one first processor in communication with said user profile database; and

a wireless device in communication with said supervisory control system, said wireless device comprising:

a memory; and

at least one second processor in communication with said memory;

said at least one first processor operative to forward said first set of coordinates to said wireless device for storage in said memory;

said at least one second processor operative in response to an attempt to establish a communication from said wireless device to another communication device:

to obtain a second set of coordinates in said specified coordinate system representative of a second geographic location corresponding to a geographic location of said wireless device; and

to determine based upon said first and second set of coordinates whether said wireless device is at a location at which use of the wireless device is restricted;

to generate a control message of a first type upon a determination that said wireless device is at a location at which the use of the wireless device is restricted; and

to generate a control message of a second type upon a determination that said wireless device is at a location at which the use of the wireless device is not restricted.

34. The system of claim 33 wherein said wireless device comprises a wireless phone.

35. The system of claim 34 wherein said wireless device comprises a device operative to communicate using a data messaging protocol.

36. A method of controlling communications between a wireless communication device and another communication device comprising the steps of:

storing within a database at least one parameter corresponding to at least one restriction on use of said wireless communication device for outgoing communications, said at least one restriction comprising at least one of a time of day restriction defining at least one time period during which an outgoing communication from said wireless communication device is not permitted, an accessibility restriction comprising at least one identifier associated with another communication device that cannot be reached from said wireless communication device, and a location restriction defining at least one location at which an outgoing communication from said wireless communication device is not permitted;

forwarding said at least one parameter from said database to said wireless communication device and storing said at least one parameter in a memory within said wireless communication device;

in response to an attempt to initiate a communication from said wireless communication device to said other communication device, retrieving said at least one parameter from said memory and determining via use of a processor within said wireless communication device, whether a connection of said communication from said wireless communication device to

said other communication device is contrary to said at least one restriction;

in the event the connection of said communication from said wireless communication device to said other communication device is not contrary to said at least one restriction, allowing the communication between said wireless communication device and said other communication device; and

in the event the communication from said wireless communication device to said other communication device phone is contrary to said at least one restriction, preventing the communication from said wireless communication device to said other communication device.

37. The method of claim 36, wherein said communication is a telephone call, said wireless communication device comprises a wireless phone, and said other communication device is another telephone and said preventing step includes the step of outputting a predetermined message for delivery to said wireless phone indicating that said call cannot be connected due to a restriction on use.

38. The method of claim 36, wherein said accessibility restriction defining at least one identifier that cannot be reached from said wireless communication device comprises a list of identifiers associated with other communication devices that are inaccessible from said wireless communication device, said method further including the steps of:

determining whether an identifier associated with said other communication device is included in said list of identifiers; and

in the event said identifier is included in said list of identifiers, preventing said communication from being completed.

39. The method of claim 37, wherein said predetermined message indicates that said other communication device associated with said identifier is inaccessible.

40. The method of claim 36, further including the step of:

determining whether an identifier corresponding to said other communication device is included in a list of identifiers that can always be reached; and

in the event the connection of said communication is contrary to a use restriction comprising one of said time, date and location restriction, and said identifier corresponding to said other communication device is included in said list of identifiers corresponding to other communication devices that can always be reached, allowing said communication between said wireless communication device and said other communication device to proceed.

41. The method of claim 36, wherein said wireless communication device comprises a wireless phone, said other communication device comprise another phone, said communication is a call from said wireless phone to said other phone, the method further including the steps of:

determining whether a predetermined allocation of time for a specified control period associated with said wireless phone has been fully depleted;

determining whether an identifier corresponding to said other phone is included in a list of identifiers associated with other phones that may always be called; and

in the event said predetermined allocation of time associated with said wireless phone has been fully depleted and said identifier corresponding to said other phone is in said

list of identifier that may always be called, connecting said wireless phone to said other phone.

42. The method of claim 36 wherein said determining step comprises the step of executing program code on said processor within said wireless device to determine whether the connection of said communication is contrary to said at least one restriction.

43. Apparatus for controlling usage of a wireless device comprising:

a first memory within said wireless device for storing at least one parameter specifying at least one restriction on use of said wireless device for outgoing communications, said at least one restriction on use comprising at least one of a time of day restriction defining times during which an outgoing communication from said wireless device is not permitted, an accessibility restriction defining at least one identifier associated with another communication device that is inaccessible for outgoing communications from said wireless device, and a location restriction defining at least one restricted location from which an outgoing communications from said wireless device is not permitted;

at least one processor within said wireless device;

a second memory operable to store program code executable on said at least one processor; and

program code stored in said second memory and executable on said at least one processor, said program code operable:

to detect the initiation of a communication from said wireless device to said other communication device and, responsive to said initiation, to determine whether a connection of said communication between said wireless

device and said other communication device is contrary to said at least one restriction;

to permit said communication from said wireless device to said other communication device in the event said connection is not contrary to said at least one restriction; and

to prevent said communication from said wireless device to said other communication device in the event said communication is contrary to at least one of said at least one restriction.

44. The apparatus of claim 43 wherein said first and second memories comprise different portions of the same memory.

45. A system for controlling usage of a wireless phone, said system operative in conjunction with a billing system including a first server operable to execute a billing process and a first database containing parameters defining billing parameters applicable to said wireless device, said system comprising:

a second server operable to execute a supervisory process for controlling usage of said wireless phone as an overlay to said billing process;

a second database containing a value defining a time duration that said wireless device may be used within a predetermined period, said second database being communicably coupled to said second server;

said second server being operative:

to maintain a record of time usage for said wireless phone within said predetermined period;

to prevent a call involving said wireless phone from being connected in the event said record of time usage indicates that said wireless phone has been used within

said predetermined period for a period equal to said time duration; and

to allow a call involving said wireless phone to be connected in the event said record of time usage indicates that said wireless phone has been used in said predetermined period for a period less than said time duration.

46. The system of claim 45 wherein said first and second servers comprise a single server operative to execute said billing process and said supervisory process.

47. The system of claim 45 wherein said first database and said second database comprise portions of a single database.

48. The system of claim 45 wherein said predetermined period comprises a calendar month and said value comprises a specified number of minutes.

49. The system of claim 45 wherein said second database includes an always accessible number associated with another communication device that may always be called by said wireless phone and said second server is operative to exclude time involving calls between said wireless phone and said other communication device from said record of time usage.

50. A computer based method of controlling the use of a wireless device comprising the steps of:

storing in a database a supervisory account identifier associated with a supervisory account, said supervisory account including information pertaining to the use of at least one wireless device including said wireless device, said

information being password protected and at least some of said information being modifiable by said account administrator;

storing in said database in association with said supervisory account identifier at the request of said account administrator, a wireless device identifier associated with said wireless device and at least one modifiable restriction governing the use of said wireless device by a wireless device user, wherein said wireless device user is an individual distinct from said account administrator;

storing in said database in association with said supervisory account identifier, a code value corresponding to a cut-through code, wherein said code-value is useable by said account administrator to permit said account administrator to establish communication with said wireless device at a time when the use of said wireless device is restricted;

receiving an indication of an intended communication from a communication device to said wireless device;

determining whether said intended communication violates said at least one restriction governing the use of said wireless device prior to connection of said communication between said communication device and said wireless device;

in the event said determining step indicates that the connection of said intended communication violates said at least one restriction and an input value corresponding to said stored code value is not received from said communication device within a predetermined time interval, generating a control message of a first type to prevent said communication from proceeding; and

in the event said determining step indicates that the connection of said intended communication would violate said at least one restriction pertaining to the use of said wireless device and said input value corresponding to said code value code is received from said communication device within said

predetermined time interval, generating a control message of a second type to allow said communication to be proceed.

51. The method of claim 50 wherein said step of storing said code value corresponding to said cut-through code comprises the step of storing in said database a user name and utilizing a value corresponding to said user name as said code value.

52. A computer based system for controlling the use of a wireless device by a wireless device user, said system comprising:

a database stored in a storage device, said database containing a supervisory account identifier associated with a supervisory account, said database including information pertaining to the use of at least one wireless device, including said wireless device, said information contained in said database being password protected and modifiable by a supervisory account administrator;

said database containing in association with said supervisory account identifier, a wireless device identifier associated with said wireless device and at least one parameter defining at least one restriction governing the use of said wireless device by said wireless device user, wherein said wireless device user is an individual distinct from said account administrator;

said database a code value corresponding to a cut-through code, wherein said code value is stored in association with said supervisory account identifier and wherein said code-value is useable by said account administrator to establish communication with said wireless device at a time when the use of said wireless device is restricted;

at least one computer operative to:

receive an indication of an intended communication from a communication device to said wireless device;

determine using said at least one parameter whether said intended communication violates said at least one restriction governing the use of said wireless device prior to connection of said communication between said communication device and said wireless device;

generate a control message of a first type to prevent said communication from proceeding in the event said at least one computer determines that the connection of said intended communication would violate said at least one restriction and an input value corresponding to said stored code value is not received from said communication device within a predetermined time interval; and

generate a control message of a second type to allow said communication to proceed in the event said at least one computer determines that the connection of said intended communication would violate said at least one restriction pertaining to the use of said wireless device and said input value corresponding to said code value code is received from said communication device within said predetermined time interval.

53. The system of claim 52 further including:

an access point and a web server communicably coupled via a data network;

a data path between said web server and said database;

said access point operative to receive as an input from said supervisory account administrator a user name and to communicate said user name to said database;

said database operative to store said user name in association with said supervisory account identifier; and

said at least one computer being operative to utilize said user name stored in said database as said code value.

54. The system of claim 53 wherein said data path includes said at least one computer.

55. A method of communicating information regarding the usage of a wireless device comprising the steps of:

storing in a database an identifier of said wireless device in association with an identifier associated with a supervisory account, wherein information in said database pertaining to said supervisory account is modifiable by a supervisor having administrative responsibility for said supervisory account;

storing in said database in association with said wireless device identifier at least one parameter defining at least one alert condition relating to the usage of said wireless device;

maintaining for said at least one wireless device a time measure indicative of the cumulative usage of said wireless device within a control period;

determining whether said alert condition has occurred by utilizing said time measure and said at least one parameter; and

in the event said determining step indicates that said alert condition has occurred, communicating an alert message to said supervisor.

56. The method of claim 55 wherein said at least one parameter includes a time value defining the amount of time said wireless device may be used prior to the transmission of said alert message to said supervisor.

57. The method of claim 56 wherein said communicating step further includes the step of communicating said alert message to said supervisor when said determining step indicates that said time measure equals said time value.

58. The method of claim 56 wherein said communicating step further includes the step of communicating said alert message to said supervisor each time said determining step indicates that said time measure equals an integral multiple of said time value within said control period.

59. The method of claim 58 further including the step of resetting said time measure at the beginning of each control period.

60. The method of claim 55 wherein said communicating step comprises the step of communicating said alert message to said supervisor via an audible message directed to a telephone number specified by said supervisor and stored in said database.

61. The method of claim 55 wherein said communicating step comprises the step of communicating said alert message to said supervisor via a text message directed to a telephone number specified by said supervisor and stored in said database.

62. The method of claim 55 wherein said communicating step comprises the step of communicating said alert message to said supervisor via an email message directed to an email address specified by said supervisor and stored in said database.

63. The method of claim 55 wherein said alert message includes an indication of said measure indicative of said

cumulative usage of said wireless device within said control period.

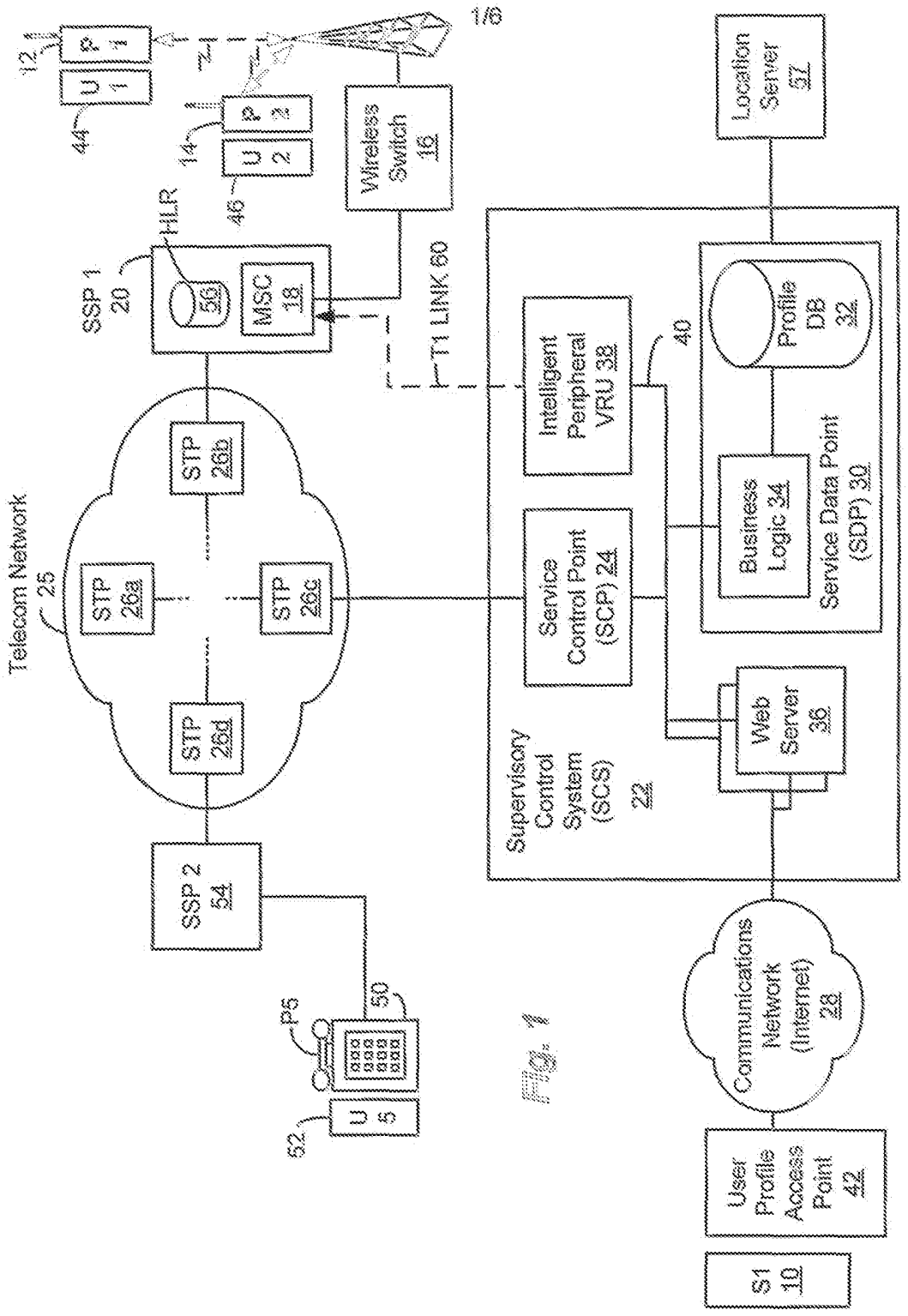

1/6
12
P 1
U 1
44
14
P 2
U 2
46
Wireless Switch 16
SSP 1 20
HLR
56
MSC 18
T1 LINK 60
Telecom Network 25
STP 26a
STP 26b
STP 26c
STP 26d
SSP 2 54
P5
50
U 5
52
Location Server 57
Intelligent Peripheral VRU 38
40
Profile DB 32
Service Control Point (SCP) 24
Business Logic 34
Service Data Point (SDP) 30
Web Server 36
Supervisory Control System (SCS) 22
Communications Network (Internet) 28
User Profile Access Point 42
S1 10

Fig. 1

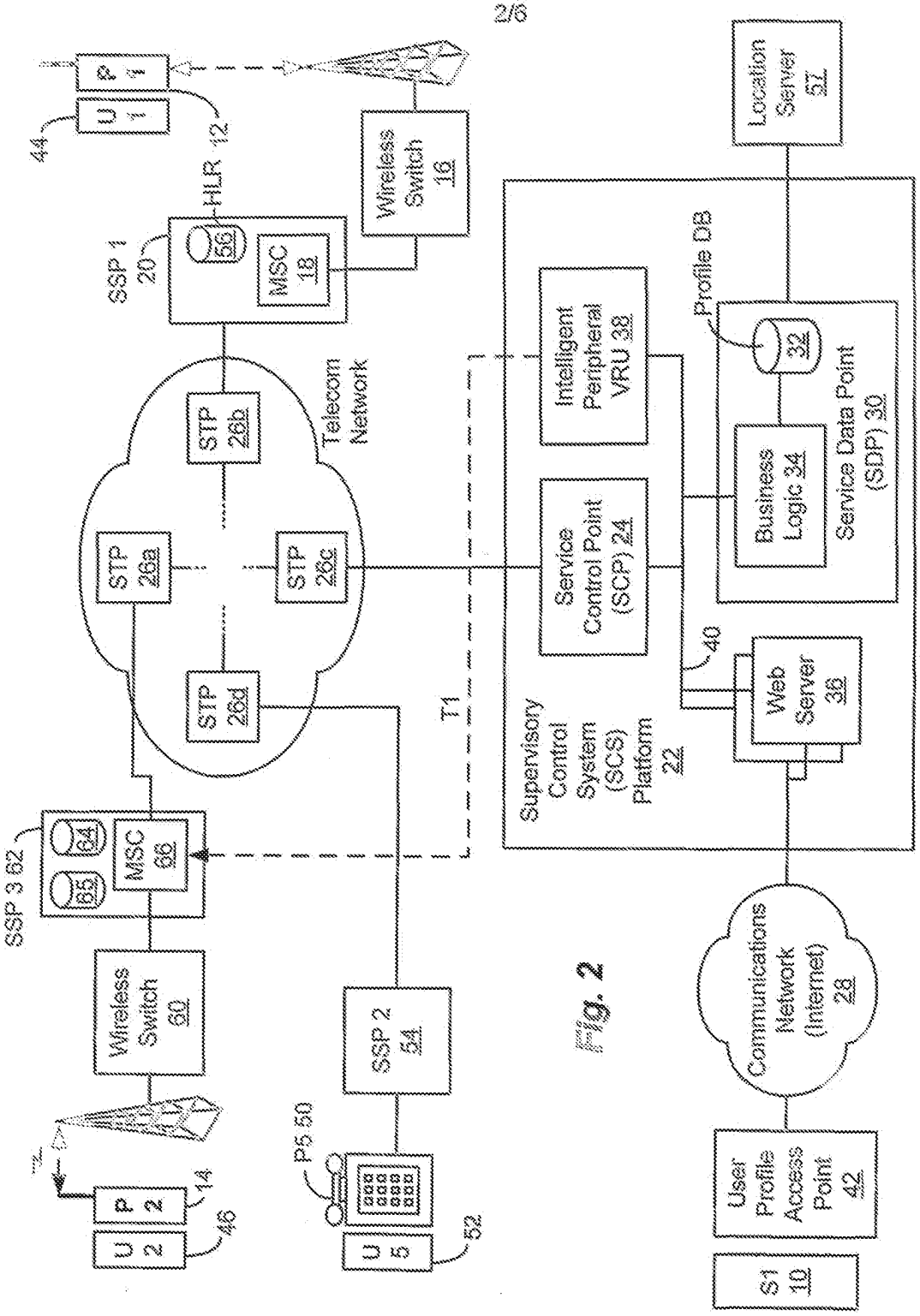

Location Server 57
Profile DB
32
Intelligent Peripheral VRU 38
Business Logic 34
Service Data Point (SDP) 30
Service Control Point (SCP) 24
Supervisory Control System (SCS) Platform 22
40
Web Server 36
T1
Telecom Network
STP 26a
STP 26b
STP 26c
STP 26d
SSP 1 20
HLR 12
59
MSC 18
Wireless Switch 16
44
U 1
P 1
SSP 3 62
64
65
MSC 66
Wireless Switch 60
SSP 2 54
P5 50
U 5
52
U 2 2
P 2 2
14
46
Communications Network (Internet) 28
User Profile Access Point 42
S1 10

Fig. 2

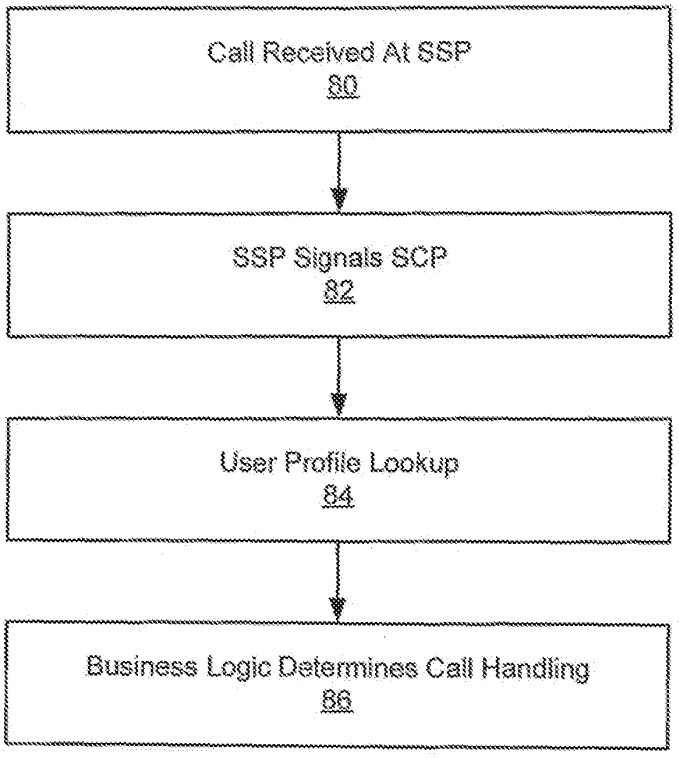

Call Received At SSP
80
SSP Signals SCP
82
User Profile Lookup
84
Business Logic Determines Call Handling
86

Fig. 3

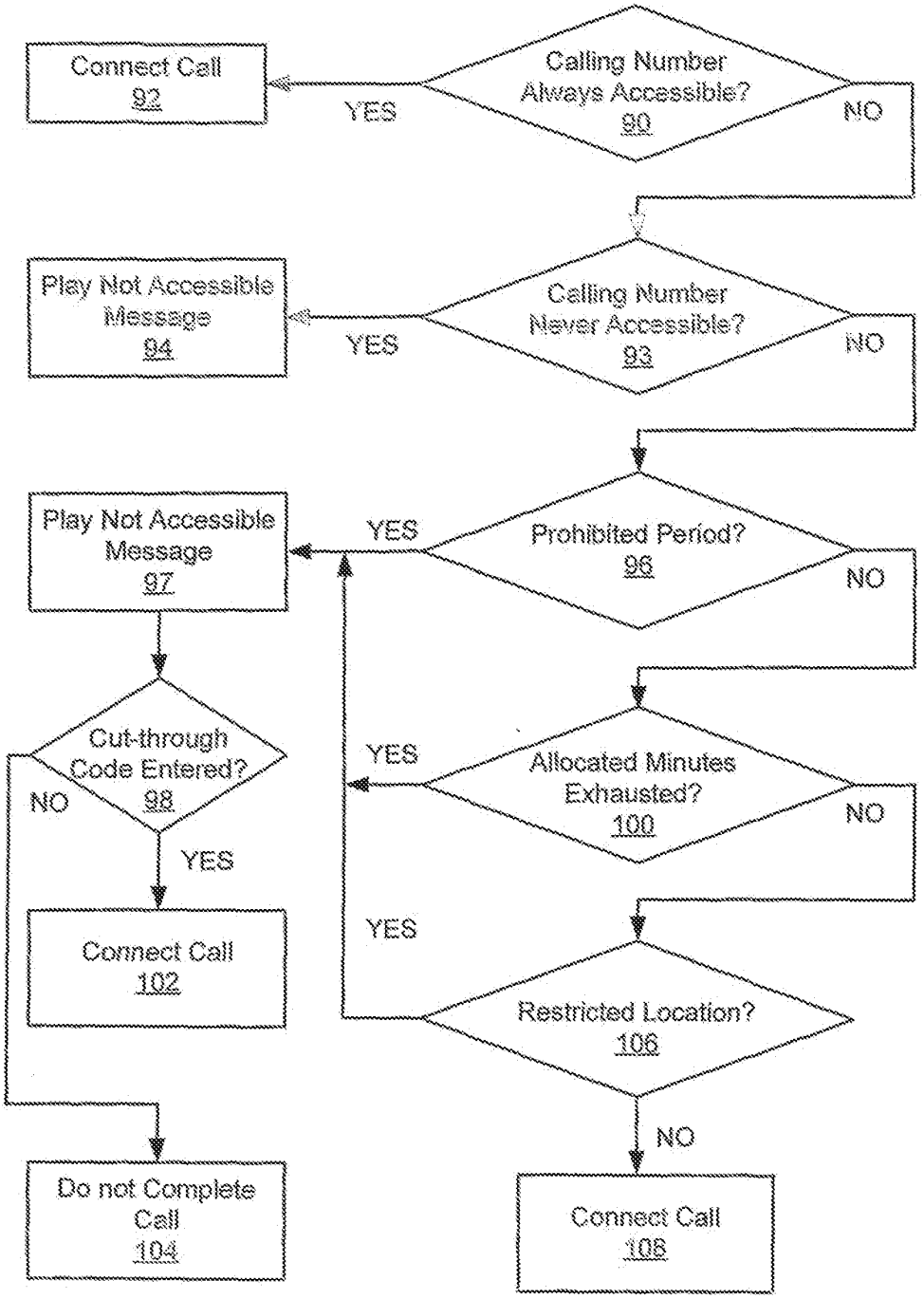

Calling Number Always Accessible? 90
YES
NO
Connect Call 92
Calling Number Never Accessible? 93
YES
NO
Play Not Accessible Message 94
Prohibited Period? 96
YES
NO
Play Not Accessible Message 97
Allocated Minutes Exhausted? 100
YES
NO
Cut-through Code Entered? 98
NO
YES
Connect Call 102
Restricted Location? 106
YES
NO
Do not Complete Call 104
Connect Call 108

Fig. 4

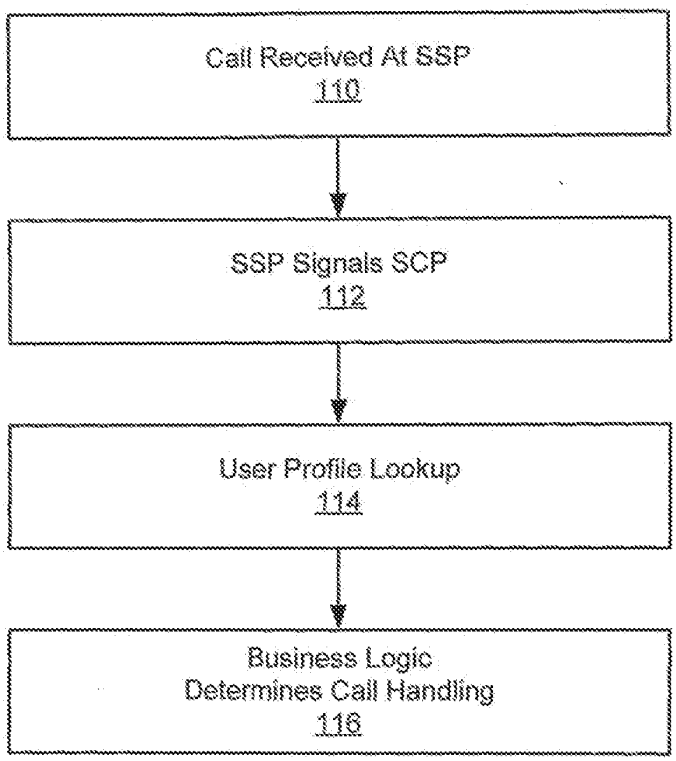

Call Received At SSP
110
SSP Signals SCP
112
User Profile Lookup
114
Business Logic
Determines Call Handling
116

Fig. 5

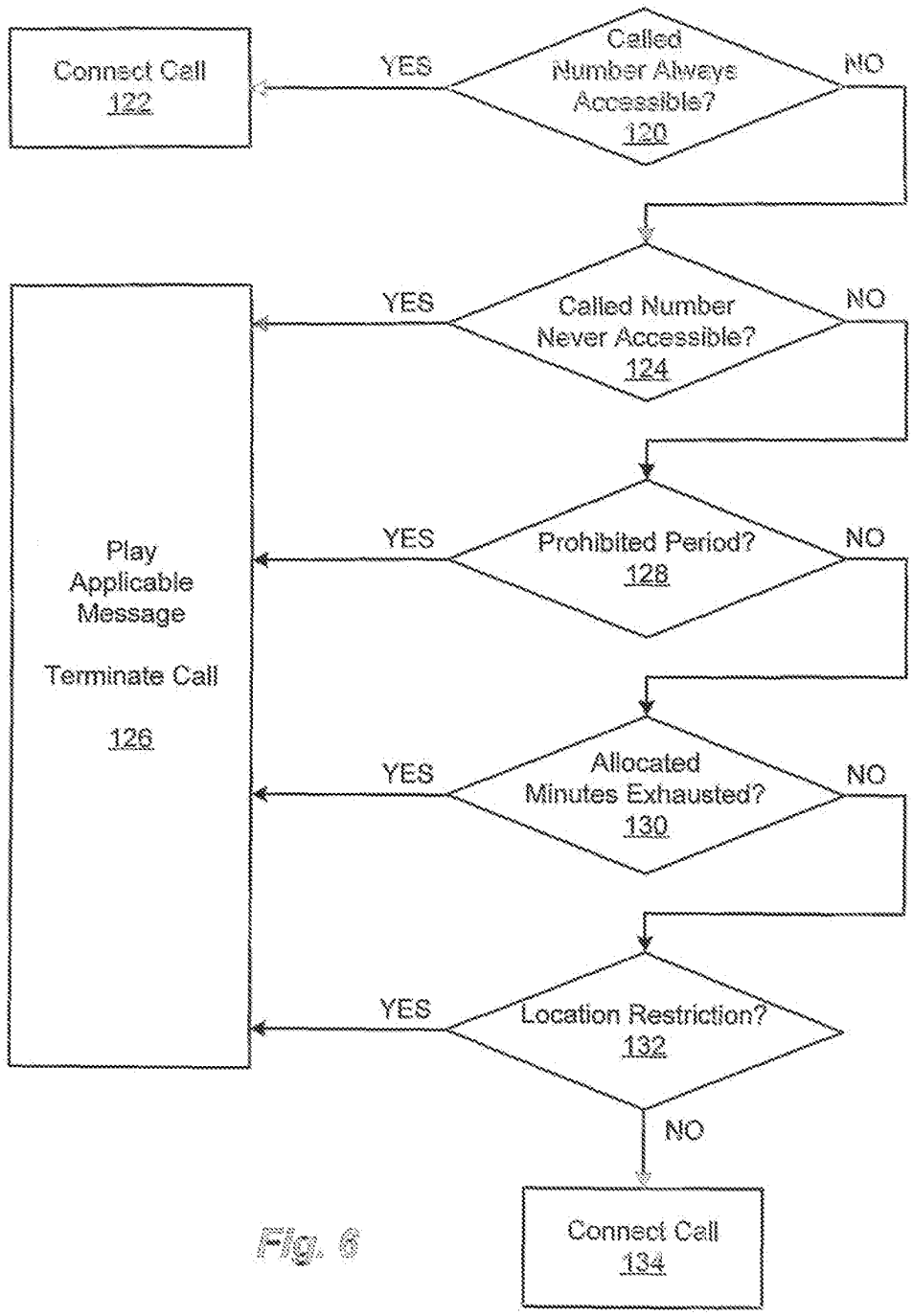

Connect Call
122
YES
Called Number Always Accessible?
120
NO
YES
Called Number Never Accessible?
124
NO
Play Applicable Message
Terminate Call
126
YES
Prohibited Period?
128
NO
YES
Allocated Minutes Exhausted?
130
NO
YES
Location Restriction?
132
NO
Connect Call
134

Fig. 6

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 July 2003 (17.07.2003)

PCT

(10) International Publication Number
WO 03/058880 A1

(51) International Patent Classification[7]: H04L 9/32, G07F 7/08

(21) International Application Number: PCT/SE02/02424

(22) International Filing Date:
20 December 2002 (20.12.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0200061-0 10 January 2002 (10.01.2002) SE

(71) Applicant *(for all designated States except US)*: **TELIA AB (publ)** [SE/SE]; Mårbackagatan 11, S-123 86 Farsta (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ERIKSSON, Jonas** [SE/SE]; John Ericssonsgatan 16, S-652 22 Karlstad (SE). **KÅWE, Rolf** [SE/SE]; Lingonstigen 7, S-654 68 Karlstad (SE).

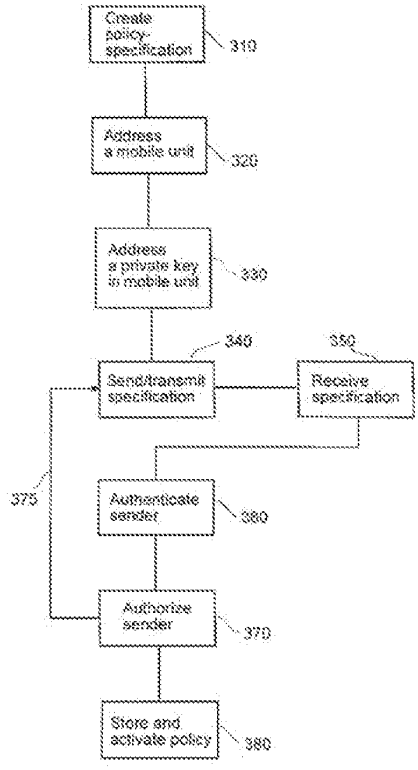
(74) Agent: **SVENSSON, Peder**; Telia Research AB, Vitsandsgatan 9, S-123 86 Farsta (SE).

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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

[Continued on next page]

(54) Title: METHOD AT ACCESS RIGHT CONTROL WITHIN MOBILE COMMUNICATION



(57) Abstract: The present invention related to a method in a mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access from a mobile terminal of a service at a service provider requires a password. The method includes the steps to: - from a service provider, or by him/her appointed certificate authority, electronically transmit/send a password policy to a mobile unit, - in a mobile unit electronically receive said policy and handle and create/configure password connected/associated with said service provider according to rules specified in, the from the service provider or by him/her appointed certificate authority, said policy. The method also includes that the mobile unit or a specific gateway authenticates and authorizes the transmitter/sender of the policy in order to prevent illegal utilization of the possibility to change a policy.

WO 03/058880 A1

ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

Published:

— *with international search report*

METHOD AT ACCESS RIGHT CONTROL WITHIN MOBILE COMMUNICATION

TECHNICAL FIELD

The present invention relates to the field access right control within mobile communication systems.

PRIOR ART

There is a number of connections/situations within a mobile radio communication system with mobile units and connected units which provide services over said communication systems, where the access from a mobile terminal of a service at such a service provider requires a password for access right control/check in a mobile unit for access to different functions, data files or for use of encryption keys. These passwords frequently can be changed by the user. Usually there is a need for certain restrictions regarding among other things configuration and validity for these passwords.

In the patent document WO 01/35685 a system to deliver a PIN-code (PIN = Personal Identification Number) to a mobile terminal by means of an SMS-message (SMS = Short Message Service) is described. The system makes it possible that a SIM-card (SIM = Subscriber Identity Module) is equipped with a PIN-code after the card having been delivered to customer.

In the patent document US 6,202,157 a system to distribute and execute a policy for password in a network for data communication is described.

In the patent document US 4,924,514 a device for handling of encryption keys is described. Control vectors control the handling of the keys at which the cryptographic facility is given possibility to change its policy.

The invention is among other things based on the knowledge of the inventors about that there usually is a need to put a policy into practice about which codes that can be selected. In order to today apply a policy for password, which is connected to local functions in the mobile unit, is required that this policy in entered into the mobile unit or additional units, for instance a smart card at, or just before, distribution of these units.

Both mobile operators and banks are interested in, and are working on, solutions where a user shall be authenticated (be identified to have declared/stated identity) and by his/her mobile unit create digital signatures which cannot be rejected. Typically the mobile unit consists of a mobile telephone with one or more so called smart cards. The mobile unit (or usually a smart card in the mobile unit) in its turn contains one or more private keys, which can be used for authentication and to create "non-rejection" only when a CA (Certificate Authority) has issued certificate which verifies that a specific user holds these private keys.

The use of the private keys are all but always protected by a password, which users often have possibility to change or select themselves. CA has in many cases points of view on which rules that shall apply for which passwords a user is allowed to select. CA then has what is generally called a password policy. The password policy can for instance apply to rules regarding length, allowed characters and updating intervals. Such a policy only has been possible to apply to the cases where it already at the issuing of the card has been made clear which CA that shall issue the certificate connected/associated to the keys on the card. In the mobile case, the smart card often will be distributed to the user before anyone knows what CA that shall issue the certificate connected/associated to pair of keys on the

card; so the method of entering/applying CA´s password policy on the card before it is distributed to the user is not applicable.

SUMMARY OF THE INVENTION

The aim of the invention is to provide a method to electronically distribute a password policy over a mobile communication system to a mobile unit so that said policy directly can start being applied in the mobile unit or an additional unit. The invention consequently includes a method within a mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access from a mobile terminal of a service at a service provider requires a password. The method includes the steps to:

- from a service provider, or by him/her appointed certificate authority, electronically transmit a password policy to a mobile unit;
- in a mobile unit electronically receive said policy and handle and draw up/configure passwords associated with/to said service provider according to rules specified in the from the service provider or by him/her appointed certificate authority, said issued/transmitted policy.

The method also includes that the mobile unit or a specific gateway authenticates and authorizes the sender of the policy in order to prevent illegal utilization of the possibility to change a policy.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described more in detail in the following, with references to enclosed drawings, in which:
Figure 1 shows an administration route/path according to one embodiment of the invention for PIN-policy.
Figure 2 shows an administration route/path for PIN-policy according to another embodiment of the invention; and

Figure 3 shows a flow chart for a method according to the invention.

Figure 4A and 4B show schematically the location/placing of authentication and authorization units according to two embodiments of the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

One embodiment of the invention relates to a method to distribute a password in form of a PIN-policy for cryptographic keys in mobile units "over the air", that is via the communication system in which the unit is intended to operate. The keys are in the typical case held/kept in a device/smart card in the mobile unit which cannot be juggled with, but it is not necessary. The cryptographic keys are in the typical case private keys in asymmetric pair of keys. The cryptographic keys, or the unit in which these are generated, have been distributed to the user already before it is known which party that will issue certificate which associates/connects the user to a certain pair of keys.

When a CA shall issue a certificate, the user is linked/associated to a private key in usual way via an "over the air proof of possession"-procedure. Before, after or during this procedure CA distributes its PIN-policy via the cellular mobile communication system to the mobile unit which holds/contains the private key. An application in the mobile unit attends to that the PIN-policy comes into force, and forces the user to select a PIN-code according to the policy for utilization of the certified key. In Figure 1 the flow is illustrated:

1. CA 101 has decided to distribute its PIN-policy to a certain mobile unit.
2. CA addresses the PIN-policy to a certain mobile unit and a certain private key in the mobile unit 115 and

transmits/sends this to a gateway 105 for the purpose. This gateway 105 authenticates CA 101 and decides whether CA 101 is entitled to distribute a PIN-policy to the mobile unit 115 (authorization). Said gateway 105 is preferably arranged at the operator of the mobile communication system.

3. Gateway 105 sends/transmits the PIN-policy further over the mobile communication network 110.
4. The mobile unit 115 receives the PIN-policy, secures that it is coming from the mobile operator's gateway 105, and activates the policy for key in question. If the user since before has a PIN-code which does not fulfil the policy, he/she is requested to select a new PIN-code according to the policy.
5. Alternatively, when the user changes PIN-code next time, it has to fulfill the requirements in the PIN-policy.

Step 1 is preferably preceded by an inquiry from the client/user to CA about issuing of a client certificate. A password policy preferably includes rules about, in the general case:

- number of characters/symbols(min., max.)
- prohibited characters/symbols
- prohibited combination of characters/symbols
- intervals for how often change of password has to be done (for instance the number of times a password is allowed to be used).

The policy of course can be general for all users, but also "personalized", for instance include controls of that a certain user does not utilizes his/her personal code number as PIN etc.

In one embodiment a PIN-policy consists of a data structure which is interpreted by an application for the purpose which has been arranged in the mobile unit. In

another embodiment a PIN-policy is realized as an executable application which is transmitted to the mobile unit. In the first case it is conceivable that a plurality of PIN-polices can be active at the same time, but some mechanism to solve conflicting policies, if any, then is needed.

The mobile unit 115 then preferably includes one or more integrated or removable smart cards or any other form of device which is protected against manipulations. The invention of course is applicable also in the cases when the private key is not stored in a device which is protected against manipulation, but in any other way in the mobile unit.

In one embodiment the specific gateway which is mentioned in step 2 does not exist, compare Figure 2. Instead CA 201 transmits its policy via a general traffic gateway for the mobile communication network (GGSN for GPRS/UMTS) 210, without mechanisms for authentication and authorization of CA 201. In this embodiment mechanisms for authentication and authorization are instead implemented in the mobile unit 215

In Figure 3 the method steps corresponding to the distribution path in Figure 1 and Figure 2 are shown. CA creates 310 a policy specification, and addresses 320 a mobile unit and addresses 330 a private key within said mobile unit. Further, the specification is transmitted 340 over the mobile network, possibly via a specific gateway as has been mentioned above. The specification is received 350 and the transmitter/sender is authenticated 360, respective, whenever applicable, authorized 370. Depending on the number of units between CA and mobile unit which need own authentication and authorization, the steps to transmit 340, receive 350, authenticate 360 and

authorize 370 are repeated 375. Finally, the policy is stored and activated in the mobile station.

Of course in alternative embodiments other parties than CA can load down a PIN-policy. Particularly in one embodiment the operator of the mobile communication service is capable of loading down his/her PIN-policy to the mobile units in his/her network.

PIN-policy for other purposes than unlocking/use of private keys of course also can be distributed to the mobile unit according to the invention. For instance PIN-codes and passwords for:

- use of symmetrical keys
- write/read rights to/of data files
- GSM
- execution of applications

etc.

In the case there are more than one CA (we call these A respective B) which certifies the same key, the following method is an embodiment of the invention:

- Both A and B can load down its policy to the mobile unit. Both policy from CA A and a policy from CA B are put into practice each time PIN is changed. This requires a mechanism in the mobile unit to solve conflicting demands.
- Both A and B sends/transmits its policy to the operator of the mobile communication network. The operator creates a "summing up" of these rules and decides about which policy that finally is transmitted to the mobile unit.
- Both A and B can load down its policy to the mobile unit. Separate PINs are used for the same key depending on which of his/her certificates the user wants to refer to. Policy from CA A applies when the

user refers to his/her certificate from CA A, and policy from CA B applies when the user refers to his/her certificate from CA B.

In Figure 4 A and B are shown how units for authentication and authorization have been arranged in preferred embodiments. Fig. 4A shows an authentication unit 402 and an authorization unit 404 arranged in gateway 105. Figure 4B shows an authentication unit 402 and an authorization unit 404 arranged in a mobile unit 115.

Of course there is in most cases a reliable transport mechanism required to transmit a PIN-policy from CA, or other provider/issuer of the policy, to the mobile unit. There are several methods to realize this, but this is out of the scope of the invention.

The scope of protection is only limited by the following patent claims.

PATENT CLAIMS

1. A method in a mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access via a specific mobile terminal of a specific service at a specific service provider requires a password, c h a r a c t e r i z e d in that said method includes the steps to

- from a service provider, or by him/her appointed certificate authority electronically transmit a password policy to a mobile unit
- in a mobile unit, electronically receive said policy and handle and create/configure password in connection with said service provider according to rules specified in, from the service provider or by him/her appointed certificate authority, said transmitted/send policy.

2. A method as claimed in patent claim 1, c h a r a c t e r i z e d in the following steps:

- creation of a password policy specification at a service provider or by him/her appointed certificate authority (CA)
- production/deriving of the address to a mobile unit,
- production/deriving of the address to a private key in said mobile unit,
- transmission/sending of the specification,
- reception of the specification,
- authentication of CA,
- authorization of CA,
- storing of a policy which corresponds to the specification, and
- activation of said policy.

3. A method as claimed in patent claim 1, c h a r a c t e r i z e d in that it includes the following steps.

- creation of a password policy specification at a CA,
- production/deriving of the address to a mobile unit,
- production/deriving of the address to a private key in said mobile unit,
- distribution of the policy specification to a gateway for downloading of policy,
- authentication of CA in said gateway,
- authorization of CA in said gateway,
- distribution of the specification from gateway to mobile unit over a mobile communication network,
- reception of the specification,
- ensuring that the specification is emanating from approved gateway,
- storing of a policy which corresponds to the specification, and
- activation of said policy.

4. A method as claimed in patent claim 3, c h a r a c t e r i z e d in that it further includes the step:

- forcing the user to immediately change password to one which fulfils the new policy.

5. A method as claimed in patent claim 3, c h a r a c t e r i z e d in that it further includes the step;

- awaiting to insert/apply the policy until the user changes password next time.

6. A method as claimed in any of the patent claims 1-5, c h a r a c t e r i z e d in that said password is a PIN-code.

7. A mobile radio communication system with mobile units and connected service providers who provide services over said communication system, where the access via a specific mobile terminal of a specific service at a specific service provider requires a password, c h a r a c t e r i z e d in that said system includes means to, from a service provider, transmit/send a policy specification for password to a mobile unit.

8. A mobile communication system as claimed in patent claim 7, c h a r a c t e r i z e d in that said system includes means to in a mobile unit receive a policy specification for password.

9. A mobile communication system as claimed in patent claim 8, c h a r a c t e r i z e d in that in said system means has been arranged for authentication of a policy sender/transmitter.

10. A mobile communication system as claimed in patent claim 8, c h a r a c t e r i z e d in that in said system means has been arranged for authorization of a policy sender/transmitter.

11. A mobile communication system as claimed in patent claim 7, c h a r a c t e r i z e d in that a gateway including means for authentication and authorization of a policy-sender/transmitter has been arranged to connect a CA to the mobile communication system, and to authorize and authenticate said CA.

12. A mobile communication system as claimed in patent claim 9 or 10, c h a r a c t e r i z e d in that means for authorization of a policy-transmitter/sender has been arranged in a mobile unit.

13. A mobile communication system as claimed in any of the patent claims 7-12, c h a r a c t e r i z e d in that said policy specification is arranged in form of a data structure.

14. A mobile communication system as claimed in any of the patent claims 7-12, c h a r a c t e r i z e d in that said policy specification is arranged in form of an executable application.

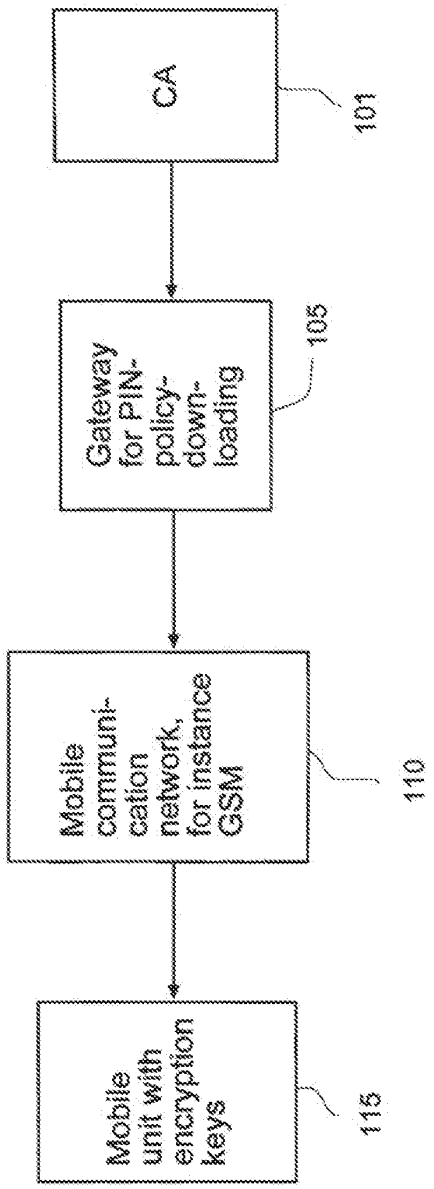

CA
101
Gateway for PIN-policy-down-loading
105
Mobile communi-cation network, for instance GSM
110
Mobile unit with encryption keys
115

Figure 1

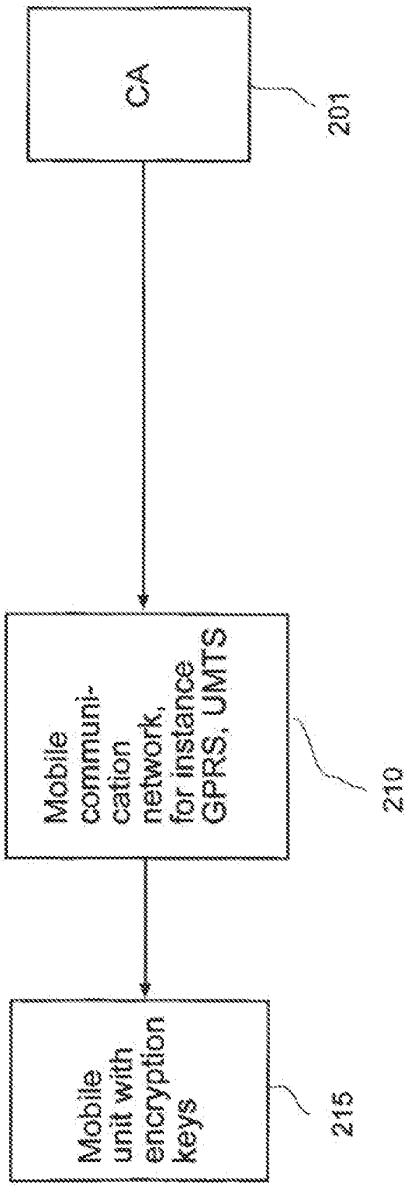

CA
201
Mobile communi-cation network, for instance GPRS, UMTS
210
Mobile unit with encryption keys
215

Figure 2

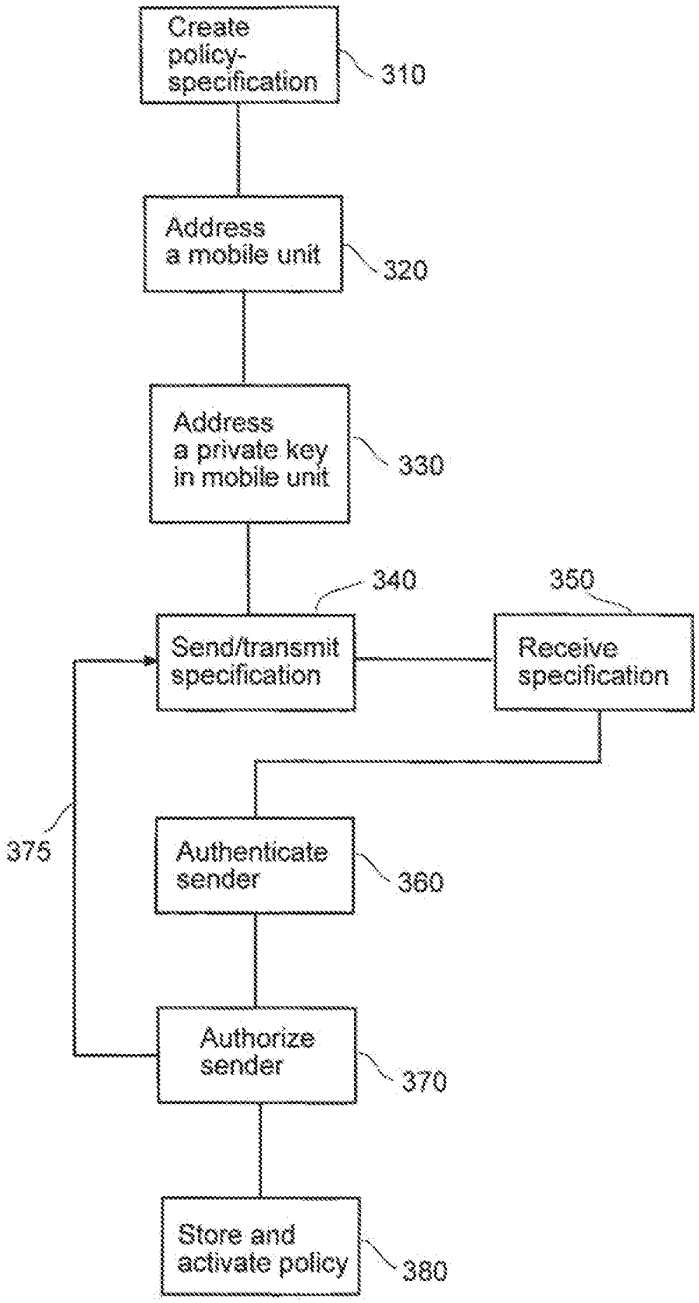

Create policy-specification
310
Address a mobile unit
320
Address a private key in mobile unit
330
340
350
Send/transmit specification
Receive specification
375
Authenticate sender
360
Authorize sender
370
Store and activate policy
380

Figure 3

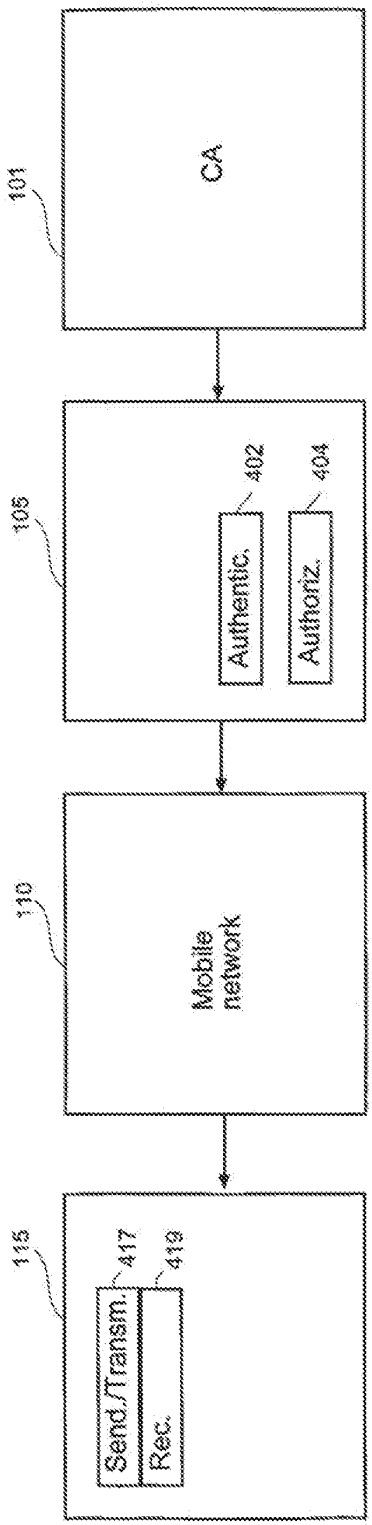


Figure 4A

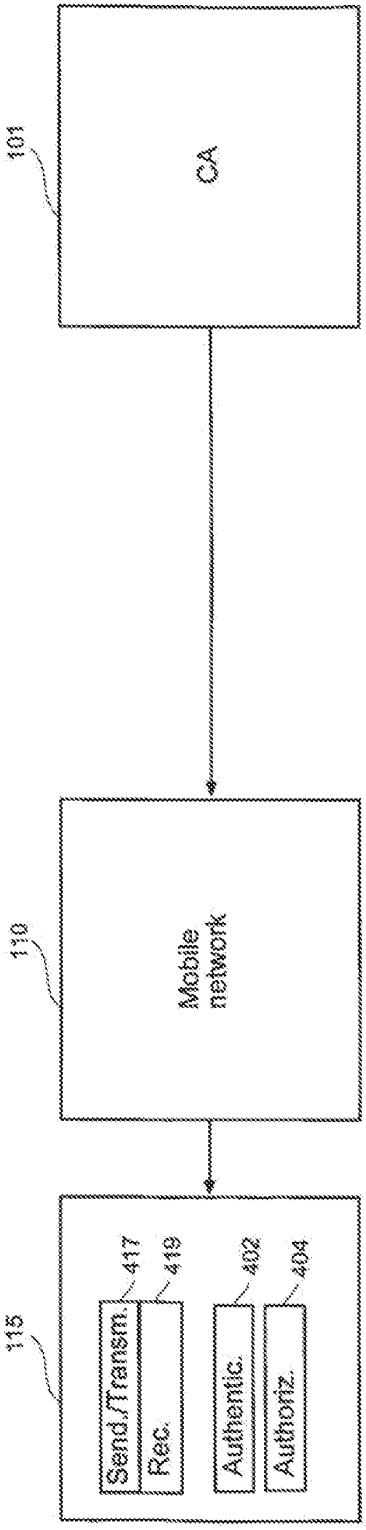


Figure 4B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/02424

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32, G07F 7/08
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)

IPC7: H04L, G06F

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6202157 B1 (BROWNLINE, M. ET AL), 13 March 2001 (13.03.01), abstract, cited in the application ---	1-14
A	WO 0135685 A1 (MOBILIX A/S), 17 May 2001 (17.05.01), abstract, cited in the application ---	1-14
A	US 5944824 A (HE, J.), 31 August 1999 (31.08.99), claim 1 ---	1-14
A	US 4924514 A (MATYAS, S.M. ET AL), 8 May 1990 (08.05.90), cited in the application ---	1-14

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"B" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 April 2003	09 -04- 2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/mj Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/02424

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0354771 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 14 February 1990 (14.02.90), abstract -- --------	1-14

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/02/03

International application No.
PCT/SE 02/02424

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6202157 B1	13/03/01	NONE	
WO 0135685 A1	17/05/01	AU 1269001 A	06/06/01
		BR 0015445 A	05/11/02
		DK 160899 A	10/05/01
		EP 1228653 A	07/08/02
US 5944824 A	31/08/99	NONE	
US 4924514 A	08/05/90	CA 1313411 A	02/02/93
		DE 68922884 D,T	30/11/95
		DE 68926005 D,T	17/10/96
		EP 0354771 A,B	14/02/90
		EP 0356065 A,B	28/02/90
		JP 2105192 A	17/04/90
		JP 2107722 C	06/11/96
		JP 8023736 B	06/03/96
EP 0354771 A2	14/02/90	CA 1317677 A	11/05/93
		DE 68922884 D,T	30/11/95
		DE 68926005 D,T	17/10/96
		DE 68926076 D,T	14/11/96
		DE 68926200 D,T	17/10/96
		EP 0354770 A,B	14/02/90
		EP 0354774 A,B	14/02/90
		EP 0356065 A,B	28/02/90
		JP 2099984 A	11/04/90
		JP 2105990 C	06/11/96
		JP 8020848 B	04/03/96
		US 4941176 A	10/07/90
		CA 1313411 A	02/02/93
		JP 2105192 A	17/04/90
		JP 2107722 C	06/11/96
		JP 8023736 B	06/03/96
		US 4924514 A	08/05/90

Electronic Acknowledgement Receipt

EFS ID:	7930889
Application Number:	12380773
International Application Number:	
Confirmation Number:	5719
Title of Invention:	Verifiable service policy inplementation for intermediate networking devices
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	21912
Filer:	Michael J. Schallop/Veronica Pula
Filer Authorized By:	Michael J. Schallop
Attorney Docket Number:	RALEP018
Receipt Date:	01-JUL-2010
Filing Date:	02-MAR-2009
Time Stamp:	13:40:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	RALEP018_IDS_Before_1st_OA.pdf	56528 360846d02c00e598c3909f3171296226f661c34e	no	2
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Filed (SB/08)	RALEP018_IDS_SB08_2.pdf	89822 3a74ec70278cc2f90ad13dc3e62514bd94c85032	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	RALE_Foreign_Ref_2A.pdf	5821505 81bd528285eeb7055e34118b1c6f3ad0b406f580	no	34
Warnings:					
Information:					
4	Foreign Reference	RALE_Foreign_Ref_2B.pdf	4014433 6c150dbecf6e07e6e926c4953d9f7fa596419ee3	no	26
Warnings:					
Information:					
5	Foreign Reference	RALE_Foreign_Ref_2C.pdf	8969766 8a08a661fedb57f7c563ba498f498bb2309c2fc6	no	61
Warnings:					
Information:					
6	Foreign Reference	RALE_Foreign_Ref_2D.pdf	12405145 775980dffc4fd87b178f106d99003d7a52ddaca2	no	79
Warnings:					
Information:					
7	Foreign Reference	RALE_Foreign_Ref_2E.pdf	2436174 c0f643662921a19d681c882cd985d04b7837a8bd	no	21
Warnings:					
Information:					
8	NPL Documents	RALE_NPL_Ref_2F.pdf	219474 ebce1f8721f1fe656f69a3905f36d944f0f575a4	no	6
Warnings:					
Information:					
9	NPL Documents	RALE_NPL_Ref_2G.pdf	682711 8ee373cfd5a9d752aae23b4ea2fc1e12b949497c	no	77
Warnings:					
Information:					
10	NPL Documents	RALE_NPL_Ref_2H.pdf	137925 312ccdc04271430ed42b709573c0105d48599e5d	no	8

Warnings:					
Information:					
11	NPL Documents	RALE_NPL_Ref_2I.pdf	1378815 1d1b86ccc61e4d602380d993e4561849720eab8b	no	17
Warnings:					
Information:					
12	NPL Documents	RALE_NPL_Ref_2J.pdf	1319237 50d69a59a8af2531967879de03d70ef081c646f2	no	5
Warnings:					
Information:					
13	NPL Documents	RALE_NPL_Ref_2K.pdf	384366 ca4acdc0719ea1636b3d667e2aafd3397dfca7ef	no	23
Warnings:					
Information:					
14	NPL Documents	RALE_NPL_Ref_2L.pdf	3636374 8440928107fdb5d75ce06783a2192520dc545702	no	15
Warnings:					
Information:					
15	NPL Documents	RALE_NPL_Ref_2M.pdf	887279 5a30977e77dc57a16d92c2240fea93e245299f94	no	111
Warnings:					
Information:					
16	NPL Documents	RALE_NPL_Ref_2N.pdf	2190991 8ba9616337a9da73d1158dfaec561ac7bc23b576	no	219
Warnings:					
Information:					
17	NPL Documents	RALE_NPL_Ref_2O.pdf	22848329 5dfb6b37b9bdba2974aea1f1643a2cc9b9129f17	no	262
Warnings:					
Information:					
18	NPL Documents	RALE_NPL_Ref_2P.pdf	496028 a267ff12b9b336818993ff8b85da8e35a5708cc5	no	35
Warnings:					
Information:					
19	NPL Documents	RALE_NPL_Ref_2Q.pdf	1970806 2398c7ca475eec3e037b4ad60021644397a754ed	no	10

Warnings:					
Information:					
20	NPL Documents	RALE_NPL_Ref_2R.pdf	347340 e87bfc75fa6949a4c1ea09d431b076cdc1b55249	no	11
Warnings:					
Information:					
			Total Files Size (in bytes):	70293048	

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

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

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Gregory G. Raleigh	Examiner:	Not Assigned
Application No.:	12/380,773	Art Unit:	2445
Filed:	March 2, 2009	Docket No.:	RALEP018
Title:	VERIFIABLE SERVICE POLICY IMPLEMENTATION FOR INTERMEDIATE NETWORKING DEVICES		

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§1.56 AND 1.97(b) BEFORE MAILING OF A FIRST OFFICE ACTION

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The references listed in the attached PTO SB/08, may be material to examination of the above-identified patent application. Applicants disclose these references in compliance with their duty of disclosure pursuant to 37 CFR §§1.56 and 1.97. The Examiner is requested to make these references of official record in this application. Copies of the cited references are provided to the extent required by 37 CFR §1.98 and any applicable waivers.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that these references indeed constitute prior art.

This Information Disclosure Statement is being filed (1) with the above-referenced application or (2) within three months of the filing date of the above-referenced application or (3) before the mailing date of a first Office Action on the merits or (4) before the mailing date of a first Office Action after filing of a Request for Continued Examination. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 50-0685 (Order No. RALEP018).

Respectfully submitted,
VAN PELT, YI & JAMES LLP

/Michael J. Schallop/

Michael J. Schallop
Registration No. 44,319
V (408) 207-4762
F (408) 973-2595

10050 N. Foothill Blvd, Ste 200
Cupertino, CA 95014

Substitute for form 1449/PTO				Complete if Known	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	12/380,773
				Filing Date	March 2, 2009
				First Named Inventor	Gregory G. Raleigh
				Art Unit	2445
				Examiner Name	Not Assigned
Sheet	1	of	1	Atty Docket No.	RALEP018

U.S. Patent Documents					
Examiner Initials	CiteNo.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS					
Examiner Initials	Cite No.	Foreign Patent Document Country Code–Number–Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	3A	WO 2007/014630	02-08-2007	Telefonaktiebolaget LM Ericsson	WO 2007/014630
	3B	WO 2006/004467	01-12-2006	Telefonaktiebolaget LM Ericsson	WO 2006/004467

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	3C	KNIGHT et al., Layer 2 and 3 Virtual Private Networks: Taxonomy, Technology, and Standardization Efforts, IEEE Communications Magazine, June 2004	
	3D	KOUTSOPOULOU et al., Middleware Platform for the Support of Charging Reconfiguration Actions, 2005	
	3E	NILSSON et al., A Novel MAC Scheme for Solving the QoS Parameter Adjustment Problem in IEEE802.11e EDCA, February 2006	
	3F	Author Unknown, Overview of GSM, GPRS, and UMTS, Chapter 2, November 4, 2008	
	3G	CHAOUCHI et al., Policy Based Networking in the Integration Effort Of 4G Networks and Services, 2004 IEEE	
	3H	ZHU et al., A Survey of Quality of Service in IEEE 802.11 Networks, IEEE Wireless Communications, August 2004	
	3I	KYRIAKAKOS et al., Ubiquitous Service Provision in Next Generation Mobile Networks, Proceedings of the 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004	
	3J	FAROOQ et al., An IEEE 802.16 WiMax Module for the NS-3 Simulator, March 2-6, 2009	
	3K	Author Unknown, HP, IP Multimedia Services Charging, A White Paper from HP, January 2006	
	3L	Author Unknown, Kindle™ User's Guide 3rd Edition, Copyright 2004-2009	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T^2 = Applicant is to place a check mark here if English language Translation is attached

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 February 2007 (08.02.2007)

PCT

(10) International Publication Number
WO 2007/014630 A1

(51) International Patent Classification:
H04Q 7/38 (2006.01) *H04M 3/42* (2006.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/EP2006/006776

(22) International Filing Date: 11 July 2006 (11.07.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05016857.4 3 August 2005 (03.08.2005) EP

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: NORRMAN, Karl [SE/SE]; Bondegatan 3b, 4 Tr, S-116 23 Stockholm (SE). BARRIGA, Luis [SE/SE]; Glidflyktsgatan 4 Bv, S-128 33 Skarpnäck (SE). HALEN, Joacim [SE/SE]; Anhaltsvägen 8, S-191 40 Sollentuna (SE).

(74) Agent: HOFFMANN . EITLE; Arabellastrasse 4, 81925 München (DE).

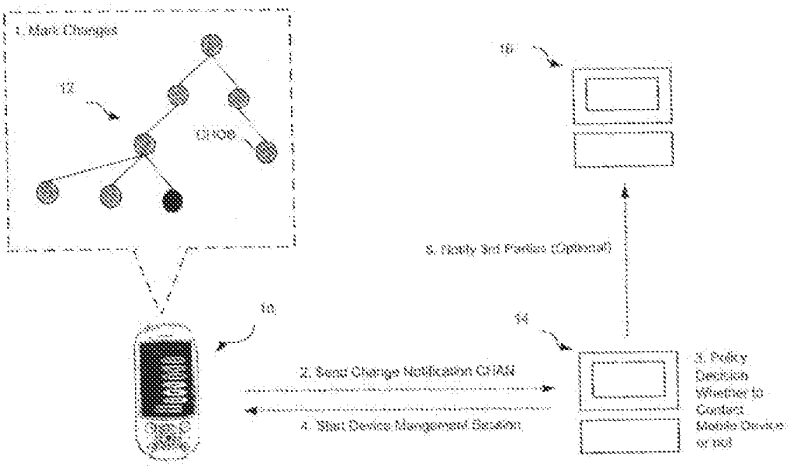
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ,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

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

Published:
— *with international search report*

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

(54) Title: AUTOMATIC MOBILE DEVICE CAPABILITY MANAGEMENT



(57) Abstract: The present invention relates to an improved approach to mobile device capability management. Heretofore, a capability management device (14) is provided at a mobile communication network. Upon change of a mobile device capability, a related notification is sent to the capability management device (14) which applies a policy decision whether to track the capability change at the network side or not. Should the decision be 'yes', the capability management device (14) starts a device management session to collect further information on a mobile device capability change beyond the information made available with the mobile device capability change notification. After retrieval of the mobile device capability change information, the capability management device (14) will update its mobile device capability state accordingly. Optionally, the capability management device (14) may share the generated information with third party (16) cooperating with the mobile device (10) for, e.g., service delivery.

WO 2007/014630 A1

Automatic Mobile Device Capability Management

FIELD OF INVENTION

The present invention relates to a method of operating a mobile device capability management apparatus in a mobile communication network and also to a method of operating a mobile device being enabled for mobile device capability management. Further, the present invention relates to a corresponding mobile device capability management apparatus and a mobile device interacting with the mobile device capability management apparatus.

BACKGROUND ART

As mobile devices are becoming more complex, flexible and capable of more functionality, each mobile device evolves into an increasingly unique user specific equipment diverging from previously pre-installed functionalities. In the telecommunication world, this leads to a big change from earlier days, when mobile devices of a certain model were static with respect to both hardware and to a large extent even software.

Today, mobile devices communicate their capabilities to a wireless communication network when attaching thereto by sending its identification ID and the version number reflecting its entire software image. Further, the operator

of the wireless communication network has the option, upon reception of the mobile device identification ID, to retrieve a stored version of the software installed in the mobile device into a mobile communication network operator controlled database.

Fig. 1 shows a sample management tree maintained in support of mobile device capability management.

One specification of such a management tree is provided by www.openmobilealliance.com and specified in OMA, SyncML device management tree and description, version 1.1, February 2002.

As shown in Fig. 1, the management tree serves to specify the structure of the configuration capability present in a mobile device. The main idea is to use the management tree, which resembles, e.g., a UNIX file system. The management tree contains sub-trees called management objects MO. These management objects are composed of information required to form a specific task, e.g., they may be related to device specific information, MMS functionality or email functionality. A device information management object contains a leaf node named './DevInfo/Lang', holding information on the currently selected operative language for the mobile device.

As shown in Fig. 1, leaf nodes may be identified using a relative unified resource identifier URI, so that it is possible to read and write content of leaf nodes using standards like Synchronization Meta language SyncML. Also, such synchronization meta languages may be used to add and remove nodes in the management tree.

Further, while it is possible for the operator to update the information in the leaves of the management tree while the mobile device is attached to the mobile communication network, there exists also the possibility to change settings and to upgrade the functionality of the mobile device from other resources than the operator of the mobile communication network. Also, this may be achieved when the mobile device is not attached to the mobile communication network. Should such a situation occur, the operator would be interested in knowing what has changed in the mobile device in order to provide such information to, e.g., service applications interacting with the mobile device or third party service providers that deliver device and their content and services to the mobile device.

Here, when a new service is made available in a mobile device, this will typically lead to a new management object being installed in the management tree. In many cases, e.g., for reasons of consistency, it would be interesting for the operator of the mobile communication network to retrieve also these extensions to the management tree. It should be noted that it is not always possible for the operator to know such information in advance.

An additional problem with existing solutions is that information conveyed by the mobile device on its capabilities is usually too coarse. As outlined above, existing solutions only provide a software version number for the entire software image present in the mobile device. Typically, such information could be sent from the access network, MSC/HLR, to a service layer device management device using automatic device detection procedures, as an example.

SUMMARY OF INVENTION

In view of the above, the object of the present invention is to provide an improved management of mobile device capabilities.

According to the present invention, this object is achieved by a method of operating a mobile device capability management device in a mobile communication network with respect to at least one mobile device served by the mobile communication network. According to the present invention, a mobile device capability is represented two-fold, i.e. as a first mobile device profile in the mobile device capability management device operated by a network operator and as a second mobile device profile maintained in the mobile device. Upon change of mobile device capability and functionality, at the mobile device capability management device, there is received a mobile device capability change information with respect to the mobile device capability change.

According to the present invention, it is suggested that the mobile device capability management device executes a step to assess the need to update the first mobile device profile in the mobile device capability management device. This assessment is achieved on the basis of a mobile device capability management policy and the received mobile device capability change information.

Therefore, the present invention provides the possibility for a mobile device capability management system run by an operator of a mobile communication network to get up-to-date information on the mobile device capability change and therefore a detailed view on the mobile device capabilities in cases where the mobile device was updated via some

facilities being different from the mobile device capability management device. Contrary to existent solutions, where only the version number of the software image is conveyed to an operator of a mobile wireless network, the present invention allows for a much finer granularity of information sent from the mobile device to a mobile device capability management device.

Further, the invention enables efficient timely automatic detection of mobile device capability changes like firmware changes or device software changes, and to retrieve information on such changes, even with respect to specific components and functionalities, e.g., an updated audio or video codec, newly installed/updated applications, and/or change of user preferences, e.g., preferred language.

According to a preferred embodiment of the present invention, there is provided the step of actually updating the mobile device profile in the mobile device capability when the assessment step indicates necessity of such an update.

Yet another important advantage of the present invention is that it is possible to execute the assessment step in a very flexible way. In other words, according to a specified mobile device capability management policy, one could, e.g., decide to track every mobile device capability change in the mobile device capability management device, or to only track such changes according to specific time windows, or with respect to certain functionalities, or according to subscriber information, whatsoever. The option to specify a mobile device capability management policy is highly advantageous to avoid unnecessary steps at the mobile device capability management device, should only minor changes occur with respect to the capability of the mobile

device. The avoidance of such unnecessary update steps at the mobile device capability management device is also a prerequisite to avoid unnecessary traffic in the mobile communication network run by the operator, which also runs the mobile device capability management device.

In more detail, according to a preferred embodiment, only upon assessment of a necessary update, there is established a mobile device management session between the mobile device capability management device and the mobile device for evaluation of the second mobile device profile in the mobile device. Then, related mobile device capability update information for processing in the mobile device capability management device is received. Preferably, such information may be provided as a mobile device management object being specified for a mobile device management tree structure which may be dedicated to the mobile device capability change management.

An important advantage of this procedure is that, as outlined above, overall mobile device management traffic can be minimized according to the established mobile device capability management policy, and that further mobile device capability change information is transferred in a way suitable for a mobile device management tree data structure used in the mobile device capability management device.

According to a preferred embodiment of the present invention, the mobile device capability change information contains a qualitative parameter indicating seriousness of change to the mobile device profile and a quantitative parameter indicating amount of detective changes to the mobile device profile.

Typically, seriousness of change reflects a degree of change or, in other words, minor, medium, major, as an example. This information is helpful to assess at the mobile device capability management device whether to actually establish a mobile device management session or not. Further, the amount of detective changes reflects the actual changes added to the mobile device profile and therefore gives information on what type of functionality has actually been changed at the mobile device side.

This two-step approach to forwarding of mobile device capability change information is very effective in that in a first step only a degree of change is indicated to the mobile device management device and then, in a second step, detailed information necessary for mobile device capability profile update at the mobile device capability management device is exchanged, e.g., by establishment of a mobile device capability management session.

According to a preferred embodiment of the present invention, the mobile device capability management device further notifies a service provider delivering services to the mobile device and/or an application interacting with the mobile device on a mobile device capability change.

An important advantage of this notification is that not only at the operator side running the mobile communication environment information reflecting a mobile device profile update is available, but also at third parties. This spread out of mobile device capability change information to all parties interacting with the mobile device achieves consistency throughout the complete operative environment and therefore an increase in quality of service delivery.

Further to the above, the object outlined above is also achieved according to a second aspect of the present invention by a method of operating a mobile device being enabled for mobile device capability management through a mobile communication network. Here, in the mobile device a mobile device capability state is represented as a mobile device profile.

According to the present invention, the method of operating a mobile device comprises the step of monitoring a change in the mobile device capability. Then, should a change in the mobile capability be monitored, there is generated a mobile device capability change information with respect to a mobile device capability change. Then, the mobile device executes a step to forward the generated mobile device capability change information to the mobile communication network. Therefore, an important advantage of the mobile device according to the present invention is that it is not only adapted to receive instructions for mobile device capability management, but that it also provides functionality in itself to continuously monitor the mobile device capability. This monitoring is a prerequisite for initiation of a capability change notification to the mobile communication network for improved mobile device capability management therein. Therefore, the operator may effectively and in real-time execute a mobile device capability update in support of back-up services for end users and/or in support of mobile device capability sharing towards external mobile device relevant applications.

According to a preferred embodiment, the mobile device capability change information comprises a qualitative parameter indicating seriousness of change to the mobile device profile and a quantitative parameter indicating amount of effective changes to the mobile device profile.

Similar to the advantages given above, the mobile device is adapted to support a two-stage approach to capability change information delivery so as to reduce traffic for mobile device capability management.

Also, it should be mentioned that according to the present invention, mobile device capability change information may be exchanged with the mobile communication network either through a circuit switched mobile communication, a packet switched mobile communication and/or through service layer data exchange or any hybrid form thereof.

Again, the applicability of different types of mobile communication support flexibility and availability of information exchange during mobile device capability management.

According to another preferred embodiment of the present invention there is provided a computer program product directly loadable into the internal memory of a mobile device capability management device in a mobile communication network comprising software code portions for performing the inventive mobile device capability management process when the product is run on a processor of the mobile device capability management device.

According to another preferred embodiment of the present invention there is provided a computer program product directly loadable into the internal memory of a mobile device being enabled for mobile device capability management through a mobile communication network comprising software code portions for performing the

inventive mobile device capability update process when the product is run on a processor of the mobile device.

Therefore, the present invention is also provided to achieve an implementation of the inventive method steps on computer or processor systems. In conclusion, such implementation leads to the provision of computer program products for use with a computer system or more specifically a processor comprised in, e.g., a mobile device capability management device or a mobile device.

This programs defining the functions of the present invention can be delivered to a computer/processor in many forms, including, but not limited to information permanently stored on non-writable storage media, e.g., read only memory devices such as ROM or CD ROM discs readable by processors or computer I/O attachments; information stored on writable storage media, i.e. floppy discs and harddrives; or information convey to a computer/processor through communication media such as network and/or Internet and/or telephone networks via modems or other interface devices. It should be understood that such media, when carrying processor readable instructions implementing the inventive concept represent alternate embodiments of the present invention.

BRIEF DESCRIPTION OF DRAWING

In the following the best mode of carrying out the present invention and corresponding preferred embodiments will be described with reference to the drawing in which:

Fig. 1 shows a sample management tree maintained in support of mobile device capability management;

Fig. 2 shows a basic concept underlying the present invention;

Fig. 3 shows a schematic diagram of a mobile device according to the present invention and a related flowchart of operation;

Fig. 4 shows a schematic diagram of a mobile device capability management device according to the present invention and a related flowchart of operation;

Fig. 5 shows a further detailed flowchart of operation for the mobile device shown in Fig. 3;

Fig. 6 shows a further detailed schematic diagram of the mobile device capability management device shown in Fig. 4;

Fig. 7 shows a detailed flowchart of operation for the mobile device capability management device shown in Fig. 6;

Fig. 8 shows an example of marking changed nodes in a mobile device management tree;

Fig. 9 shows a further example of marking changed nodes in a mobile device capability management tree; and

Fig. 10 shows examples of paths for conveying mobile device capability change information between the mobile device and the mobile device capability management device.

DESCRIPTION OF BEST MODE AND PREFERRED EMBODIMENTS

In the following, the present invention will be described with respect to what is considered as best mode and preferred embodiments thereof. While in the following different principles underlying the present invention will be explained with respect to a mobile device capability management tree, nevertheless, it should be noted that the application of such a mobile device capability management tree is not to be considered as restricting the scope of the present invention, as long as any type of information reflecting the capability of the mobile device is maintained. Thus, it should be understood that any other

type of data structure suitable for maintaining a mobile device capability profile is well covered by the present invention.

Further, insofar as different functionality of the present invention is explained, it should be clear that any such functionality may be implemented in hardware or software and/or a combination thereof.

Fig. 2 shows a basic concept underlying the present invention.

As shown in Fig. 2, in a mobile device 10, there is maintained some type of information reflecting the mobile device capability which is shown in the form of a mobile device capability management tree 12 in Fig. 2. This structure forms the pre-requisite for implementing the present invention at the mobile device side, i.e. the execution of a marking phase. Here, during changes to the mobile device capability, the mobile device monitors such changes, collects information on changes and sets up mobile capability change information that may be conveyed to the mobile device capability management device, e.g., a device management server.

As shown in Fig. 2, a second element of the inventive mobile device management is a so-called notification phase, wherein the mobile device notifies the mobile device capability management device 14 on the device capability change(s). Preferably, this notification may include the

type of change and, optionally, a descriptor of the involved mobile device capability changes.

As shown in Fig. 2, a third element of the inventive mobile device management process is a so-called reaction phase, where the mobile device capability management device 14 receives the notification of a mobile device capability change and reacts accordingly. Such reaction is based on the received mobile device capability change information and a mobile device capability management policy. Here, it should be noted that such a policy reflects how accurate the changes of mobile device capability must be tracked at the mobile device capability management device, on what mobile device capability management traffic on the network would be acceptable, type of change and related handling of the mobile device capability management device 14, etc. Also, it should be noted that according to the present invention, such a mobile device capability management policy may either be static and predetermined or dynamically changed over time.

As shown in Fig. 2, a positive assessment on necessity of a mobile device capability profile update at the mobile device capability management device 14, the mobile device capability management device 14 will react through establishing a device management session with the mobile device 10 for subsequent receipt of information being related to the mobile device capability change in any appropriate form. Optionally, the mobile device capability management device 14 may notify third parties of the mobile

device capability change, once the related information is received from the mobile device 10.

Therefore, the basic concept underlying the present invention allows for a finer granularity of information being related to a mobile device capability change which is sent from the mobile device 10 to the mobile device capability management device 14. Contrary to existing solutions, only a version number of a software image is conveyed to the operator of the mobile communication network. The present invention enables automatic detection of mobile device capability changes and subsequent retrieval of information on changes made to specific components, e.g., an updated codec, an installed application, and/or change of the user preference such as a preferred language. Therefore, the operator of the mobile communication network can use this detailed knowledge on the mobile device capability for device services for end users and/or for mobile device capability sharing towards third parties 16 and further applications.

In the following, further details of the present invention will be explained with respect to Figs. 3 to 10. Here, Fig. 3 shows a schematic diagram of a mobile device according to the present invention and a related flowchart of operation.

As shown in Fig. 3, the mobile device 10 comprises a mobile device memory unit 18, a mobile device profile monitoring unit 20, a profile changing information generating unit 22, and a communication unit 24.

Operatively, the mobile device profile monitoring unit 20 executes a step S10 to monitor a change in the mobile device capability. Further, operatively the mobile change information generating unit 22 executes a step S12 to generate mobile device capability change information with respect to a mobile device capability change. Then, the communication unit 24 executes a step S14 to forward the mobile device capability change information to the mobile communication network. Any type of information reflecting the mobile device capability is stored in the mobile device profile memory unit 18.

Fig. 4 shows a schematic diagram of a mobile device capability management device 14 according to the present invention and a related flowchart of operation.

As shown in Fig. 4, the mobile device capability management device 14 comprises a communication unit 26, an assessment unit 28, and a mobile device profile updating unit 30.

As shown in Fig. 4, operatively, the communication unit 26 executes a step S16 to receive a mobile device capability change information with respect to a mobile device capability change from a mobile device 10 being enabled for mobile device capability management. Then, operatively the assessment unit 28 will execute a step S18 to assess the need to update the mobile device profile in the mobile device capability management device. This assessment is based on a mobile device capability management policy and the received mobile device capability change information. The mobile device capability management policy, either

static or changed dynamically over time, may reflect any criteria of value to the operator of the mobile communication environment, e.g., amount of desired mobile device management traffic, degree of changes at the mobile device side, e.g., minor, middle, major, focus on specific types of functionality updates at the mobile device side of particular relevance to the operator, e.g., update of speech coding software or lower layer communication software, etc. As shown in Fig. 1, should the assessment step S18 lead to a result that no update of a mobile device profile is necessary at the time being at the mobile device capability management device 14, then the operation of the mobile device capability management device 14 stops. Otherwise, the mobile device profile updating unit 30 will react to the information received with respect to a mobile device capability change.

Fig. 5 shows a further detailed flowchart of operation of the mobile device 10 being enabled for mobile device capability management shown in Fig. 3.

As shown in Fig. 5, the mobile device profile monitoring unit 20 shown in Fig. 3 continuously executes the step S10 to monitor changes in mobile device capability. It may be implemented as a set of functions that are initiated upon a change of a mobile device profile. After step S10 the mobile device profile monitoring unit 20 executes a step S20 to check whether a change in capability in detail has occurred. If this is not the case, it will branch back to the monitoring step S10 to repeat the monitoring of mobile device capability changes. Otherwise, the profile change

information generating unit 22 executes the step S12 to generate the mobile device capability change information as outlined above. Here, without restricting the scope of the present invention, one may assume that the mobile device profile is represented as a mobile device capability management tree. Further, according to the present invention, it is suggested that the management tree contains an object called 'changes object' CHOB. For each capability change in the mobile device 10, therefore the related changes object in the management tree will be modified to reflect the changes to the mobile device capability into the changes object. From the viewpoint of a management tree representation, the changes object may reflect, when another object is changed, added or deleted, or when a change to a leaf node of the management tree has happened, as will be explained in more detail with respect to Fig. 8 and 9, respectively.

As shown in Fig. 5, after generation of the mobile device capability change information, e.g., related update of the changes object CHOB, then the communication unit 24 will execute the step S14, as soon as the mobile device has network connectivity, to forward mobile device capability change information to the mobile device capability management device 14. This may be achieved by set-up of a modification notification CHAN message. Preferably, the change notification CHAN message consists of two parts:

- A *qualitative* parameter indicating the degree of changes to the management tree. E.g., the qualitative parameter may be qualified into major, medium or

minor. Otherwise, one may consider a qualitative parameter being scaled from 0 to 1 to have a finer grid of indicating of the amount of changes.

- The second parameter is a *quantitative* parameter indicating the amount of effective changes to the management tree. Here, one may consider, e.g., a situation where an end user modified, e.g., a speech codec of a mobile device 10. Assuming that the speech codec is indeed activated, the quantitative parameter would indicate one changed node in the management tree. Otherwise, assuming that the speech codecs envisaged by the end user is not compatible with the operative system of the mobile device 10 and would therefore not be activated, the quantitative parameter would indicate an amount of 0 with respect to this change, notwithstanding the further amendments to the management tree, which may be notified at the same time with the change notification CHAN message.

As shown in Fig. 5, further steps of operation of the mobile device 10 may relate to the interaction with the mobile device capability management device 14 shown in Fig. 4.

As shown in Fig. 5, the communication unit 24 of the mobile device 10 may execute a step 822 to receive a request for mobile device capability change information from the mobile communication network, which information would be more detailed over the change notification CHAN message referred to above. Then, the communication unit 24 executes a step

S24 to establish a mobile device capability management communication session with the mobile device capability management device 14.

Then, the communication unit 24 will execute a step S26 to forward detailed mobile device capability change information to the mobile device capability management device 14. This detailed information is set up by the profile change information generating unit in cooperation with a mobile device profile memory unit 18 and the mobile device profile monitoring unit 20.

Fig. 6 shows a further detailed schematic diagram of the mobile device capability management device 14 explained with respect to Fig. 4.

As shown in Fig. 6, the mobile device profile updating unit 30 shown in Fig. 4, according to the present invention, divides into a session initiation unit 32, a change information processing unit 34, and a mobile device profile memory 36.

Fig. 7 shows a further detailed flowchart of operation for the mobile device capability management 14 shown in Fig. 6.

As shown in Fig. 7, the communication unit 26 will execute a step S28 to monitor whether a mobile device capability change information, e.g., a change notification message CHAN, has been received at the mobile device capability management device 14. If so, the assessment unit 28 will execute the step S18 to assess the need to update a mobile

device profile in the mobile device capability management device 14. In more detail, when the mobile device capability management device 14 is in receipt of a change notification message CHAN, the assessment unit 28 will retrieve the device mobile stored in the mobile device profile memory 36. Assessing the quantitative and qualitative indicators in the change notification message CHAN in relation to the retrieved device profile, the assessment unit 28 may assess the need to contact the mobile device 10 for related mobile device profile update, e.g., by modifying the management tree with respect to the mobile device 10.

E.g., in the assessment step S18, there is only a minor change to the mobile device capability. The mobile device capability management device 14 may decide to not contact the mobile device 10. However, should there be changes to critical objects in the management tree of the mobile device which touch operator policies or third party service providers, then the operator may choose to scan the mobile device 10 as soon as possible.

As shown in Fig. 7, heretofore the communication unit 26 will execute a step S32 to establish a mobile device management session with a mobile device 10 for retrieval of further detailed information on a mobile device capability change. The same communication unit 26 will execute a step S34 to receive detailed mobile device capability change information from the mobile device 10, e.g., according to a changes object CHOB. Should the mobile device capability management device 14 decide to contact the mobile device

10, it should then receive information on the CHOB object and the management tree itself in order to obtain necessary details about changes done to the management tree. In view of the above, it becomes clear that the approach according to the present invention may be basically divided into a marking phase, a notification phase, and a reaction phase. In particular, qualifiers used within the change notification CHAN message are used to prevent the mobile device capability management device from scanning the whole mobile device 10 for changes, each time the mobile device 10 is upgraded without involvement of the mobile device capability management device 14. Therefore, the present invention avoids time-consuming, unnecessary update procedures, disturbance of normal mobile device operation, generation of heavy traffic in the mobile communication network, and in particular with respect to mobile communication where cellular bandwidth is a very limited resource.

Then, the change information processing unit 34 will execute a step S36 to update the mobile device profile, e.g., a management tree, according to the received information and initiate a related update of the corresponding information in the mobile device profile memory 36. Optionally, the change information processing unit 34 may execute a step S38 to notify an information on a mobile device profile update to a service provider or in application delivery services.

In the following, further details handling mobile device capability changes will be explained with respect to Figs. 8 and 9.

According to the present invention, for the setup of mobile device capability change information, it is suggested to compute a short description of the component and capability with respect to hardware and/or software that have changed since the left time related information was notified to the operator of a mobile device capability management device. The short description can then be communicated to the mobile device capability management device.

Heretofore, the present invention solves the problem to transfer mobile device capability change information with respect to a management tree shown in Fig. 8. The state of the management tree can change according to two ways: Nodes in the management tree can be added or removed and/or the content of a node in the management tree can change. The present invention handles both cases.

In the following, there will be described a method for retrieving changes of the contents of a leaf node in the management tree. Then will follow a method that allows to detect the deletion and insertion of nodes in the management tree. Heretofore, the following notation will used:

* bit-string - a sequence of bits with most significant bit first
* internal node - a node that is not a leaf

- c[i] denotes bit number I of bit-string c
- | denotes concatenation

In the following, there will basically be described three phases. A first phase is provided to decide what mobile device capability change information needs to be conveyed to the mobile device capability management device, which phase will be referred to as mark-up of change nodes and computation of a code word. A second phase relates to the processing of information submitted by the mobile device 10 to the mobile device capability management device 14 and the related reaction thereto, which will be referred to as system side parsing in the following. A third phase, intermediate to the first phase and the second phase, is related to the way the mobile device capability change information is exchanged from the mobile device 10 to the mobile device capability management device 14.

In the following, the first phase, i.e. mark-up of changed nodes and computation of a code word, will be explained.

Heretofore, it is assumed that in the mobile device there is maintained a management tree having a management object CHOB inserted thereto. Here, the mobile device capability change information needs to convey the changes in the management object to the mobile device capability management device 14. One option is to code this information to a bit-string c referred to as code word in the following. To compute the code word, the profile change information generating unit 22 shown in Fig. 3 may follow

different strategies, which will be explained in the following.

Firstly, the mobile device profile monitoring unit 20 shown in Fig. 3 needs to detect which changes have been made to the management object CHOB since the last time a code word c was sent to the mobile device capability management device 14, i.e. a difference between the management object CHOB at a current time and a mobile device capability systems view at the network side according to a previous time of mobile device capability management. One way of achieving this is to keep a copy or a representation of a previous management tree T' in the mobile device profile memory unit 18 shown in Fig. 3, which management tree T' was used to compute a last code word. Upon the time of computing a new code word, the mobile device profile monitoring unit 20 will compare the current management tree T with the stored representation of a previous management tree T' and mark the nodes that differ. Another approach would be that the mobile device profile monitoring unit 20 marks the nodes at the time of change, e.g., if a speech codec functionality is updated to a new version. Then, the corresponding node would be flagged as changed during the update process.

With respect to the first phase, following the mark-up of changed nodes if the profile change information generating unit 22 uses the representation of the management tree with marked change nodes and computes the code word c for transmission to the mobile device capability management device 14. The code word can be computed by the profile

change information generating unit 22 in several ways, as will be explained in the following.

Heretofore, one may assume that there has been a change in the contents of one or more nodes in the management tree, but no addition or deletion of one or more nodes in the management tree. To compute the code word, the profile change information generating unit 22 initially lets the code word be an empty string and start at the root of the management tree T, which will then be traversed in the following manner:

1. If this node is an internal node, then go to step 2.
1a. If the content of this node has changed, then c=c|1.
1.b. If the content of this node has not changed, then c=c|0.
1c. End of recursion branch.
2. For each of the children of this node execute the procedure recursively.

It should be understood that if there is no specified order enforced on the children of one node in the management tree, then step 2 referred to above might be ambiguous. To avoid this, it is suggest to specify an order on the nodes of the management tree, e.g., a lexicographical order of the unified resource identifiers URI identifying each node. The code word c resulting from the execution of the given procedures hands bit-string c[0]|c[1]|c[2]| ... |c[n-1], where n is the number of the leaves in the management tree, and c[i](0<=i<n) is equal to a value of 1 when the content of the node i has changed and 0 otherwise.

One example of the procedure outlined above is shown in Fig. 8. For this example, all shaded nodes are unchanged, but the black nodes have been marked as changed by the mark-up procedure. In part **a** of Fig. 8, the first leaf is encountered, it has not changed, so that the code word is set to 0. In part **b** of Fig. 8, the next code is encountered, it has not changed either, so a value of 0 is appended to the code word, yielding 00. In part **c** of Fig. 8, a node which is marked as changed is encountered, so that the code word is accordingly set to c=001. The recursion will then proceed to the right branch of the management tree and examine that the leaf node of this branch has not changed, part **d** and **e** of Fig. 8, so that at the end of the traversal the final code word is c=0010.

The second phase is then related to the code word set-up along the line explained above handled at the mobile communication network side. When the mobile device capability management device 14 receives the code word c from the mobile device 10, it will retrieve its current view of the management tree T' from the mobile device profile memory 36 shown in Fig. 6. Here, the change information processing unit 34 will first set a counter i to 1 traverse the management tree T' in the same order which was followed by the mobile device 10, as explained with respect to Fig. 8. Each time the change information processing unit 34 visits a leaf node of the management tree T', it looks at the corresponding value c[i] of the code word. If the related value is equal to 1, the change information processing unit 34 marks the corresponding node

as changed and increases the counter i by 1 and proceeds with the traversal. If the related value c[i] is equal to 0, a counter is increased by 1 and the traversal is continued. When the change information processing unit 34 has executed the traversal of the tree and has looked at all bits of the code word, the change information processing unit may then trigger a command to read the corresponding nodes marked as changed from the management tree maintained at the mobile device 10.

In the following, further modifications of the first and second phase, i.e. marking of changed nodes at the mobile device 10 and computation of a code word, followed by system side parsing will be explained. Instead of sending the code word c to the mobile device capability management device 14, the mobile device 10 may choose to send a hash of the code word c to keep the mobile device capability change message short and/or of fixed length. Then, the mobile device capability management device 14 would keep a pre-computed list of hashes in the mobile device profile memory 36, and further a one-to-one mapping between which nodes have changed and the set of hashes that would correspond thereto. Here, the hash value should be shorter than the code word, which might give raise to collisions, i.e. if there are several possible node-change configurations corresponding to a single hash value. However, there might be several of the configurations that are not possible, e.g., some nodes may not be changed in the management tree or only be changed by the operator of the mobile communication network, so that this problem may be easily overcome. Optionally, for long code words one may

also apply a compression scheme to reduce amount of traffic in the mobile communication network.

While above it has been explained that the code word c contains one bit per leaf in the management tree, it may also be possible to reduce the length of the code word by skipping bits of those nodes that are known to have a static content. E.g., on most mobile devices it may not be possible to upgrade the screen, and in that case, the scree size of pixels could be skipped as an example. The pre-requisite is that both the mobile device 10 and the operator of the mobile communication network take the same viewpoint that the nodes are static.

Further, while above only tree traversal algorithms have been given as example, in the most general manner it is important that the management data structure is traversed in the same order by the mobile device 10 and the mobile device capability management device 14.

In the following, with respect to Fig. 9, there will be given another example for generation of mobile device capability change information with respect to the detection of additional deletion of nodes. Heretofore, a slightly different code c can be constructed.

As shown in Fig. 9, instead of only assigning a bit to each leaf node of the management tree, the profile change information generating unit 22 now assigns a bit to each node in the management tree. The value of the bit is assigned as follows: If the node has no new children or

does not have any children removed, the value of the bit associated with the node is 0, otherwise it is 1. The assignment of the bits is performed during a marking process as described above.

Heretofore, the mobile device profile monitoring unit 20 traverses the management tree using, e.g., a breadth first search, and output the bit assigned to each node when the node is visited. Also, mobile change information generating unit 22 must not traverse any new sub-trees, but only mark the parent new sub-trees with a value of 1.

Fig. 9 shows an example of the approach so far. Here, the code word computed using a breadth first search for the management tree would lead to a code word c=00010000. The order of the nodes using the breadth first search is generated by the profile change information generating unit 22 reading the nodes in the management trees top-down, left-to-right.

Then, when the mobile device capability management device 14 receives the code word, it will be scanned by the exchange information processing unit 34 from left to right, following the management tree, as shown in Fig. 9. Here, the change information processing unit 34 should use the same tree traversal algorithm as it was used by the profile change information generating unit 22 in the mobile device. If the change information processing unit 34 processes a node of which the corresponding bit in the code word is 1, this will be marked for further investigation. Once the change information processing unit 34 has executed the

scanning of the code word c, it then issues a command to the mobile device 10 for traversal of the marked nodes and pick-up of any changes that have occurred to the related children nodes. While it would of course be possible to read from the mobile device 10 during a scan, it is important to not include the newly found or to remove the deleted nodes from the management tree before the scan is complete.

The advantage of the approach explained above is that it is not necessary to read all nodes of the management tree in the mobile device 10 for upgrade of a management tree in the mobile device capability management device 14. Only sub-trees that are new or have been deleted need to be visited.

In the following, the third phase being related to exchange of mobile capability change information between the mobile device and the mobile device capability management device 14 will be explained with respect to Fig. 10.

As shown in Fig. 10, the mobile device capability change information and/or related change message CHAN can be communicated using traditional cellular signaling S87, such as automatic device detection MSC-Home Location Register HLR-Device Management Server. Depending on the bandwidth available the granularity of the mobile device profile change information may be adapted.

As shown in Fig. 10, it is also possible to convey such mobile device capability information upon GPRS attachment

using a RADIUS, 'Remote Authentication Dial In User Service', RFC2138, IETF, April 1997 / DIAMETER, 'Diameter Base Protocol', RFC3588, IRTF, September 2003 message as an attribute value from the basic GPRS support node GGSN to the AAA unit and then further to the device management GMS. Further, the mobile device can convey the mobile device capability change information via the service layer, e.g., upon start of an open mobile alliance device management session according to MTREE, OMA, SyncML Device Management Tree and Description, version 1.1, February 2002.

While with respect to Fig. 10 the application of a cellular network signaling of a GPRS/PS network and/or the service layer has been described, these processes are to be considered as examples only, and any other suitable approach to information exchange may be applied within the framework of the present invention.

CLAIMS

1. Method of operating a mobile device capability management device (14) in a mobile communication network with respect to at least one mobile device (10) served by the mobile communication network, wherein a mobile device capability is represented as first a mobile device profile in the mobile device capability management device and as a second mobile device profile in the mobile device, comprising the steps:

   - receiving (S16) a mobile device capability change information with respect to a mobile device capability change;

   - assessing (S18) the need to update the first mobile device profile on the basis of a mobile device capability management policy and the received mobile device capability change information.

2. Method according to claim 1, ***characterized in that*** it comprises a step of updating (S36) the first mobile device profile according to the mobile device capability management policy and the mobile device capability change information.

3. Method according to claim 2, ***characterized in that*** the step of updating the first mobile device profile comprises the steps:

- establishing (S32) a mobile device management session between the mobile device capability management device and the mobile device for evaluation of the second mobile device profile with respect to a mobile device capability change; and

- receiving (S34) the mobile device capability update information from the mobile device in accordance with an evaluation result.

4. Method according to one of the claim 1 to 3, ***characterized in that*** the first mobile device profile and/or the second mobile device profile is represented as a mobile device management tree structure comprising mobile device management objects.

5. Method according to claim 4, ***characterized in that*** the step of updating the first mobile device profile in the mobile device capability management device comprises a step of updating a mobile device capability change object (CHOB), wherein the mobile device capability change object is a mobile device management object in the mobile device management tree structure dedicated to mobile device capability change management.

6. Method according to one of the claims 1 to 5, ***characterized in that*** the mobile device capability change information (CHAN) contains a qualitative parameter indicating seriousness of change to the second mobile device profile and a quantitative parameter indicating amount of effective changes to the second mobile device profile.

7. Method according to claim 6, ***characterized in that*** the step of assessing (S18) the need to update the second mobile device profile is achieved through classification of the quantitative parameter and/or the qualitative parameter.

8. Method according to one of the claims 1 to 7, ***characterized in that*** it comprises a step of notifying (S38) a service provider providing at least one service to the mobile device and/or an application interacting with the mobile device on a mobile device capability change.

9. Method according to one of the claims 1 to 8, ***characterized in that*** mobile device capability change information is received directly from the mobile device at the mobile device capability management device (14).

10. Method according to one of the claims 1 to 8, ***characterized in that*** mobile device capability change information is received from a mobile device capability monitoring device.

11. Method according to one of the claims 1 to 10, ***characterized in that*** the mobile device capability change information is exchanged through circuit switched mobile communication, packet switched mobile communication, and/or through service layer data exchange.

12. Method of operating a mobile device (10) being enabled for mobile device capability management through a mobile communication network, wherein a mobile device

capability state is represented in the mobile device as a mobile device profile, comprising the steps:

- monitoring (S10) a change in the mobile device capability;

- generating (S12) mobile device capability change information with respect to a mobile device capability change;

- forwarding (S14) the mobile device capability change information to the mobile communication network.

13. Method according to claims 12, ***characterized in that*** the mobile device capability change information comprises a qualitative parameter indicating seriousness of change to the mobile device profile and a quantitative parameter indicating amount of effective changes to the mobile device profile.

14. Method according to claim 12 or 13, ***characterized in that*** it comprises the steps:

- receiving (S22) a request for detailed mobile device capability change information from the mobile communication network;

- establishing (S24) a mobile device management session with the mobile communication network; and

- forwarding (S26) the detailed mobile device capability change information to the mobile communication network.

15. Method according to one of the claims 12 to 14, ***characterized in that*** it comprises a step of representing the mobile device profile as a mobile device management tree structure comprising at least one mobile device management object.

16. Method according to claim 15, ***characterized in that*** it comprises a step of representing the mobile device capability change information as a mobile device capability change object (CHOB) in the mobile device management tree, wherein the mobile device capability change object (CHOB) is a mobile device management object in the mobile device management tree structure dedicated to mobile device capability change management.

17. Method according to one of the claims 12 to 16, ***characterized in that*** the mobile device capability change information is forwarded to a mobile device capability management device (14) in the mobile communication network.

18. Method according to one of the claim 12 to 16, ***characterized in that*** the mobile device capability change information is forwarded to a mobile device capability monitoring device in the mobile communication network, for subsequent conveyance thereof to a mobile device capability management device (14) in the mobile communication network.

19. Method according to one of the claims 12 to 19, ***characterized in that*** the mobile device capability change information is exchanged with the mobile communication network through circuit switched mobile

communication, packet switched mobile communication, and/or through service layer data exchange.

20. Mobile device capability management device (14) being operated in a mobile communication network with respect to at least one mobile device (10) served by the mobile communication network, wherein a mobile device capability is represented as a first mobile device profile in the mobile device capability management device and as a second mobile device profile in the mobile device, comprising:

- a communication unit (26) adapted to receive mobile device capability change information with respect to a mobile device capability change;

- an assessment unit (28) adapted to assess the need to update the first mobile device profile on the basis of a mobile device capability management policy and the mobile device capability change information.

21. Mobile device capability management device according to claim 20, ***characterized in that*** it comprises a mobile device profile updating unit (30) adapted to update the first mobile device profile according to the mobile device capability management policy and the received mobile device capability change information.

22. Mobile device capability management device according to claim 21, ***characterized in that*** the mobile device profile updating unit (30) comprises:

- a session initiating unit (32) adapted to initiate a mobile device management session

between the mobile device capability management device and the mobile device for evaluation of the second mobile device profile with respect to a mobile device capability change; and

- a capability change information processing unit (34) adapted to process the mobile device capability change information from the mobile device in accordance with an evaluation result.

23. Mobile device capability management device according to one of the claim 20 to 22, ***characterized in that*** it comprises a mobile device profile memory (36) adapted to store the first mobile device profile and/or the second mobile device profile according to a mobile device management tree structure comprising mobile device management objects.

24. Mobile device capability management device according to claim 23, ***characterized in that*** the capability change information processing unit (34) is adapted to update the first mobile device profile in the mobile device profile memory by updating a mobile device capability change object, wherein the mobile device capability change object (CHOB) is a mobile device management object in the mobile device management tree structure dedicated to mobile device capability change management.

25. Mobile device capability management device according to one of the claims 20 to 24, ***characterized in that*** the assessment unit (28) is adapted to process mobile device capability change information containing a qualitative parameter indicating seriousness of change to the second mobile device profile and a quantitative

parameter indicating amount of effective changes to the second mobile device profile.

26. Mobile device capability management device according to claim 25, ***characterised in that*** the assessment unit (28) is adapted to assess the need to update the second mobile device profile through classification of the quantitative parameter and/or the qualitative parameter.

27. Mobile device capability management device according to one of the claims 20 to 26, ***characterised in that*** the mobile device profile updating unit (30) is adapted to notify a service provider (16) providing at least one service to the mobile device and/or an application interacting with the mobile device on a mobile device capability change.

28. Mobile device capability management device according to one of the claims 20 to 27, ***characterised in that*** communication unit (26) is adapted to receive the mobile device capability change information directly from the mobile device.

29. Mobile device capability management device according to one of the claims 20 to 27, ***characterised in that*** communication unit (26) is adapted to receive the mobile device capability change information from a mobile device capability monitoring device.

30. Mobile device capability management device according to one of the claims 20 to 29, ***characterised in that*** the communication unit (26) is adapted to receive the mobile device capability change information through circuit switched mobile communication, packet switched

mobile communication, and/or through service layer data exchange.

31. Mobile device (10) being enabled for mobile device capability management through a mobile communication network, wherein a mobile device capability state is represented in the mobile device as a mobile device profile, comprising:

- a mobile device profile monitoring unit (20) adapted to monitor a change in the mobile device capability;

- a profile change information generating unit (22) adapted to generate mobile device capability change information with respect to a mobile device capability change;

- a communication unit (24) adapted to forward the mobile device capability change information to the mobile communication network.

32. Mobile device according to claims 31, ***characterized in that*** the profile change information generating unit (22) is adapted to generate the mobile device capability change information with a qualitative parameter indicating seriousness of change to the mobile device profile and a quantitative parameter indicating amount of effective changes to the mobile device profile.

33. Mobile device according to claim 31 or 32, ***characterized in that*** the communication unit (24) is adapted to:

- receive a request for update of a remote mobile device profile being maintained in the mobile communication network;

- establish a mobile device management session with the mobile communication network; and to

- forward detailed mobile device capability change information to the mobile communication network.

34. Mobile device according to one of the claims 31 to 33, ***characterized in that*** it comprises a mobile device profile memory unit (18) adapted to store the mobile device profile as a mobile device management tree structure comprising at least one mobile device management object.

35. Mobile device according to claim 34, ***characterized in that*** the profile change information generating unit (22) is adapted to generate mobile device capability change information as a mobile device capability change object in the mobile device management tree, wherein the mobile device capability change object is a mobile device management object in the mobile device management tree structure dedicated to mobile device capability change management.

36. Mobile device according to one of the claims 31 to 35, ***characterized in that*** the communication unit (24) is adapted to forward the mobile device capability change information to a mobile device capability management device in the mobile communication network.

37. Mobile device according to one of the claim 31 to 35, ***characterized in that*** the communication unit (24) is

adapted to forward the mobile device capability change information to a mobile device capability monitoring device in the mobile communication network, for subsequent conveyance thereof to a mobile device capability management device (14) in the mobile communication network.

38. Mobile device according to one of the claims 31 to 37, ***characterized in that*** the communication unit (26) is adapted to exchange mobile device capability change information with the mobile communication network through circuit switched mobile communication, packet switched mobile communication, and/or through service layer data exchange.

39. Computer program product directly loadable into the internal memory of a mobile device capability management device (14) operated in a mobile communication network, comprising software code portions for performing the steps of one of the claims 1 to 11, when the product is run on a processor of the mobile device capability management device.

40. Computer program product directly loadable into the internal memory of a mobile device (10) being enabled for mobile device capability management through a mobile communication network, comprising software code portions for performing the steps of one of the claims 12 to 19, when the product is run on a processor of the mobile device.

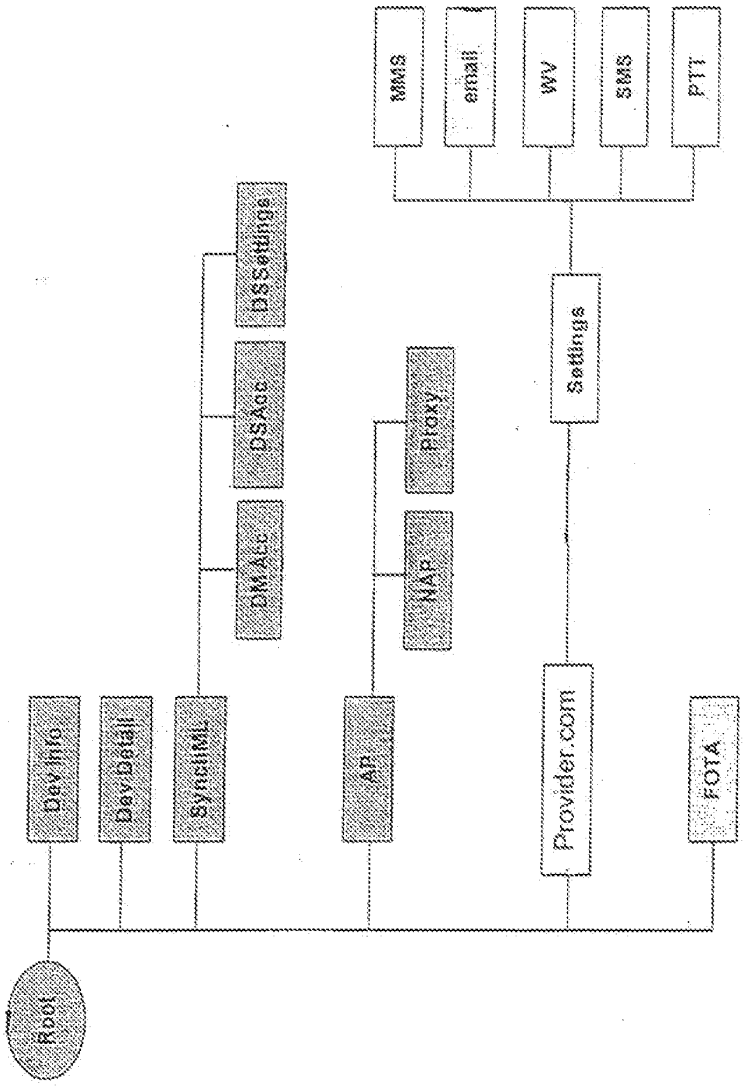

MMS
email
WV
SMS
PTT
DSSetting
DSAcc
DMAcc
Proxy
NAP
Settings
DevInfo
DevDetail
SyncML
AP
Provider.com
FOTA
Root

Fig. 1

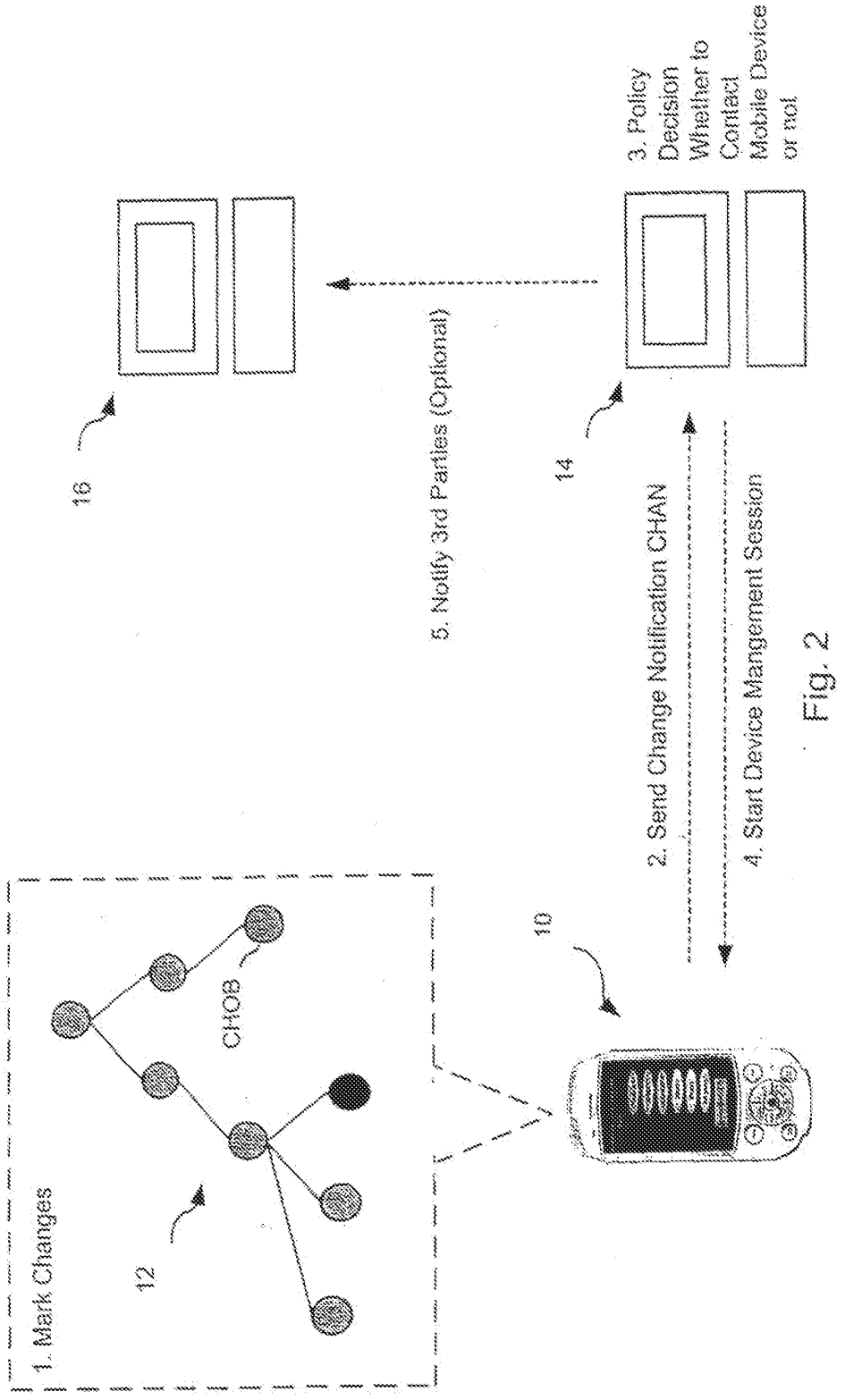

1. Mark Changes
12
CHOB
10
2. Send Change Notification CHAN
4. Start Device Mangement Session
14
3. Policy Decision Whether to Contact Mobile Device or not
5. Notify 3rd Parties (Optional)
16

Fig. 2

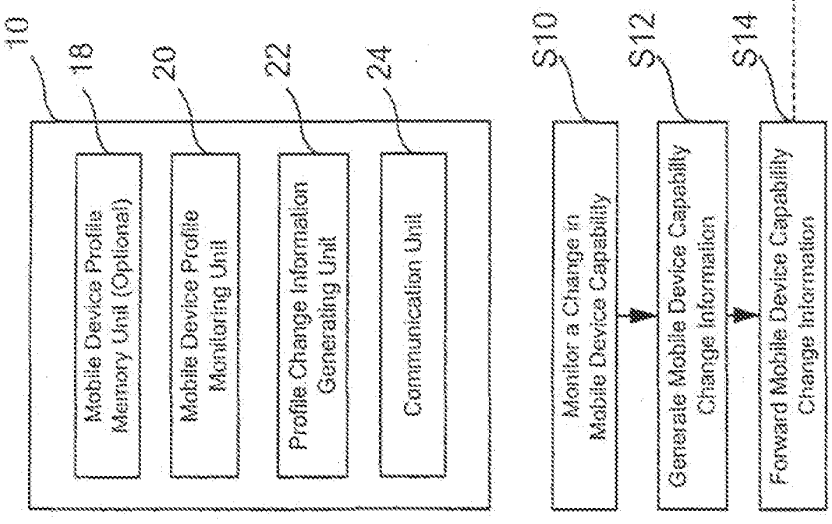

10
18
20
22
24
Mobile Device Profile Memory Unit (Optional)
Mobile Device Profile Monitoring Unit
Profile Change Information Generating Unit
Communication Unit
S10
S12
S14
Monitor a Change in Mobile Device Capability
Generate Mobile Device Capability Change Information
Forward Mobile Device Capability Change Information

Fig. 3

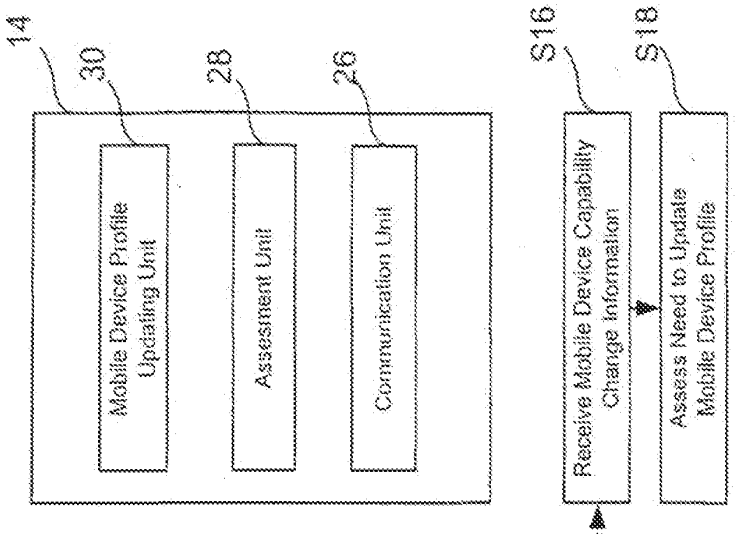

14
30
28
26
Mobile Device Profile Updating Unit
Assessment Unit
Communication Unit
S16
S18
Receive Mobile Device Capability Change Information
Assess Need to Update Mobile Device Profile

Fig. 4

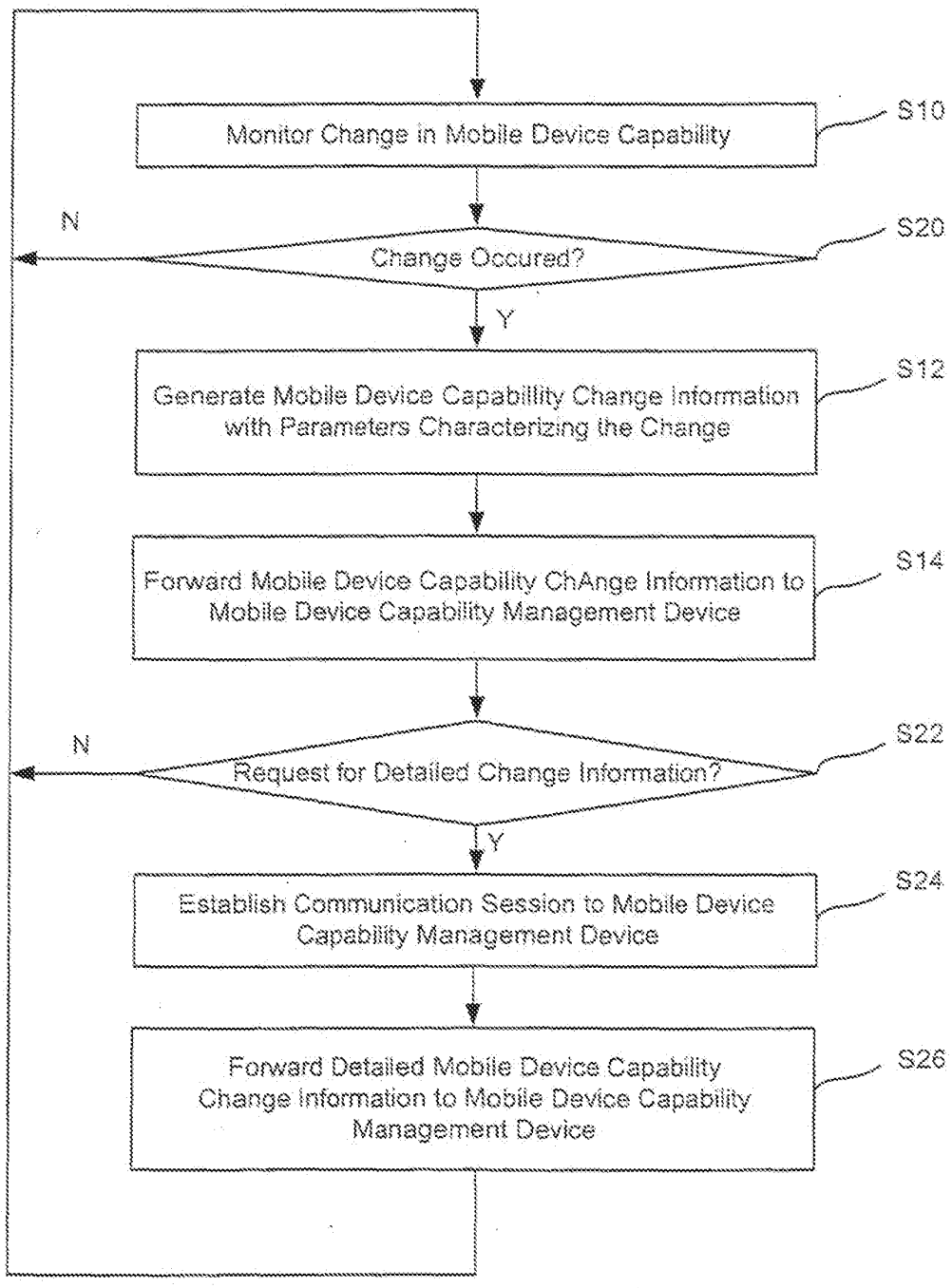

Monitor Change in Mobile Device Capability
S10
N
Change Occured?
S20
Y
Generate Mobile Device Capabillity Change Information with Parameters Characterizing the Change
S12
Forward Mobile Device Capability ChAnge Information to Mobile Device Capability Management Device
S14
N
Request for Detailed Change Information?
S22
Y
Establish Communication Session to Mobile Device Capability Management Device
S24
Forward Detailed Mobile Device Capability Change Information to Mobile Device Capability Management Device
S26

Fig. 5

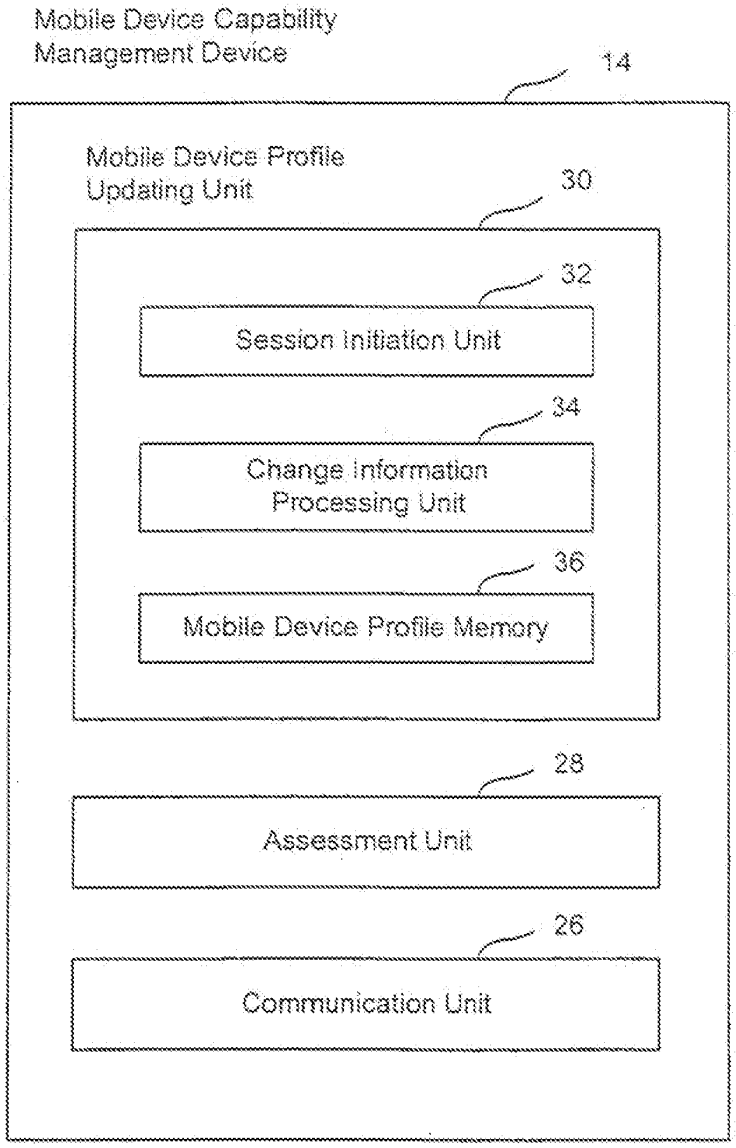

Mobile Device Capability Management Device
14
Mobile Device Profile Updating Unit
30
32
Session Initiation Unit
34
Change Information Processing Unit
36
Mobile Device Profile Memory
28
Assessment Unit
26
Communication Unit

Fig. 6

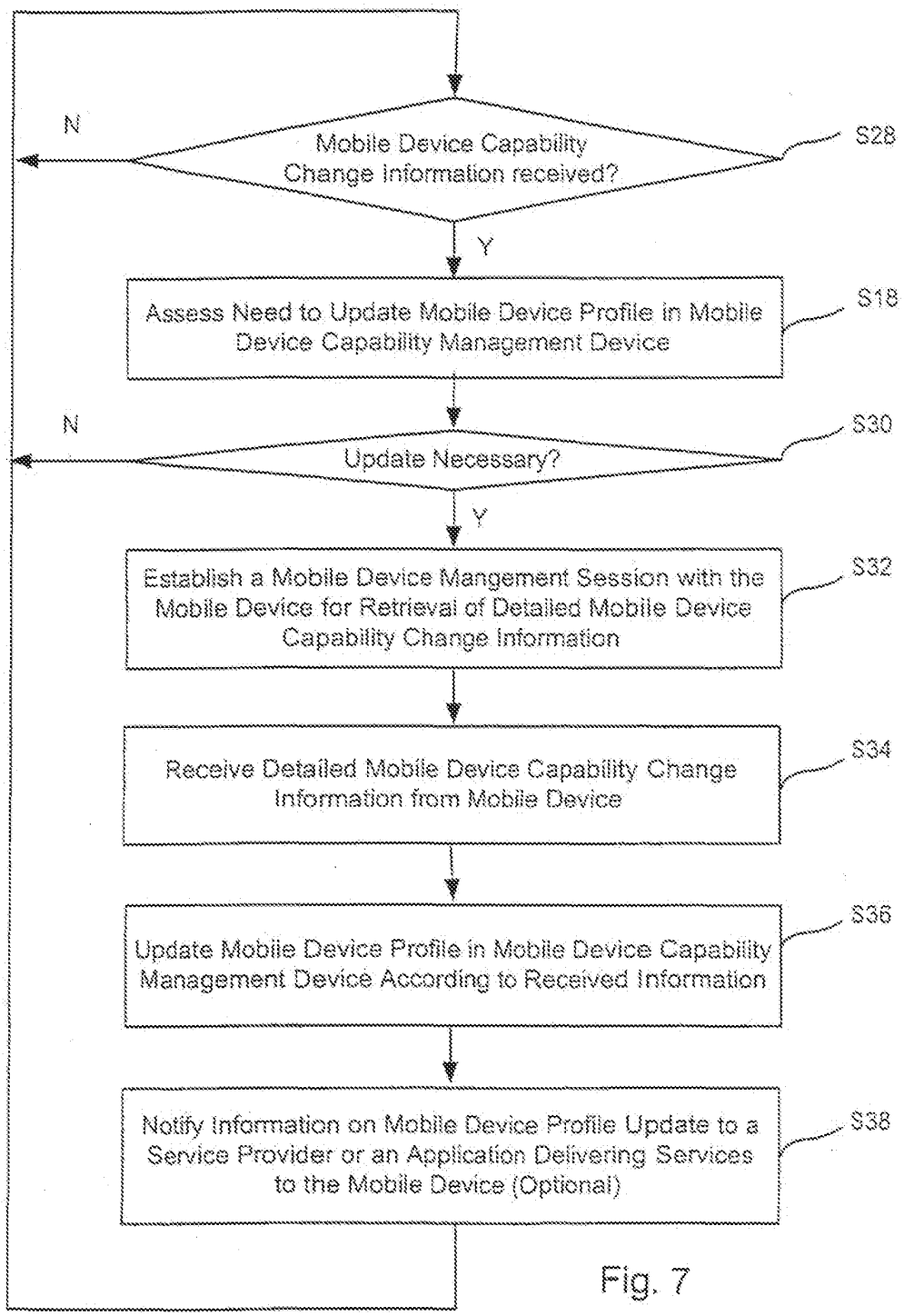

Mobile Device Capability Change Information received?
S28
N
Y
Assess Need to Update Mobile Device Profile in Mobile Device Capability Management Device
S18
Update Necessary?
S30
N
Y
Establish a Mobile Device Mangement Session with the Mobile Device for Retrieval of Detailed Mobile Device Capability Change Information
S32
Receive Detailed Mobile Device Capability Change Information from Mobile Device
S34
Update Mobile Device Profile in Mobile Device Capability Management Device According to Received Information
S36
Notify Information on Mobile Device Profile Update to a Service Provider or an Application Delivering Services to the Mobile Device (Optional)
S38

Fig. 7

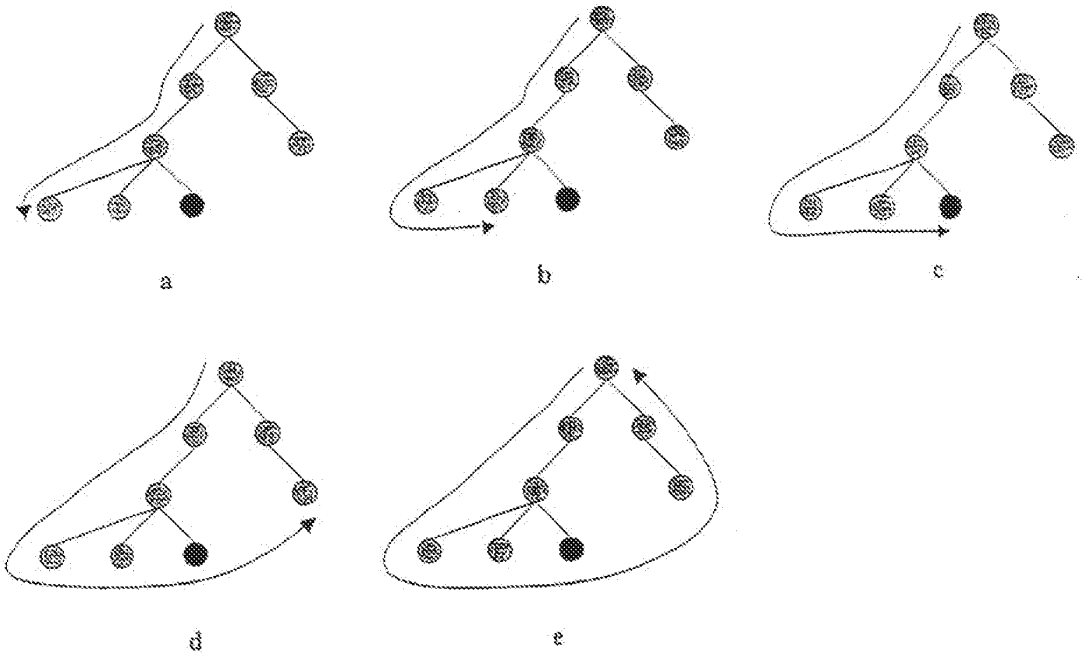


Fig. 8

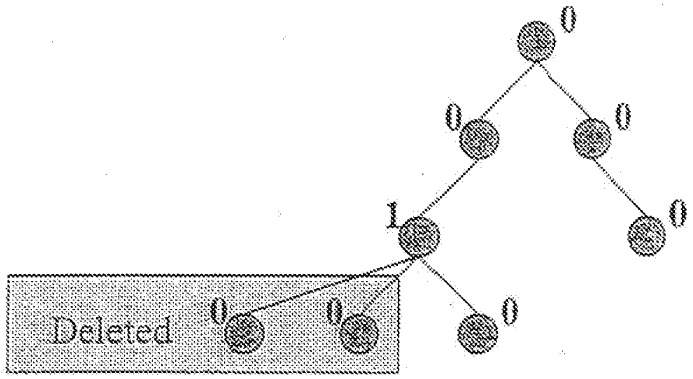


Fig. 9

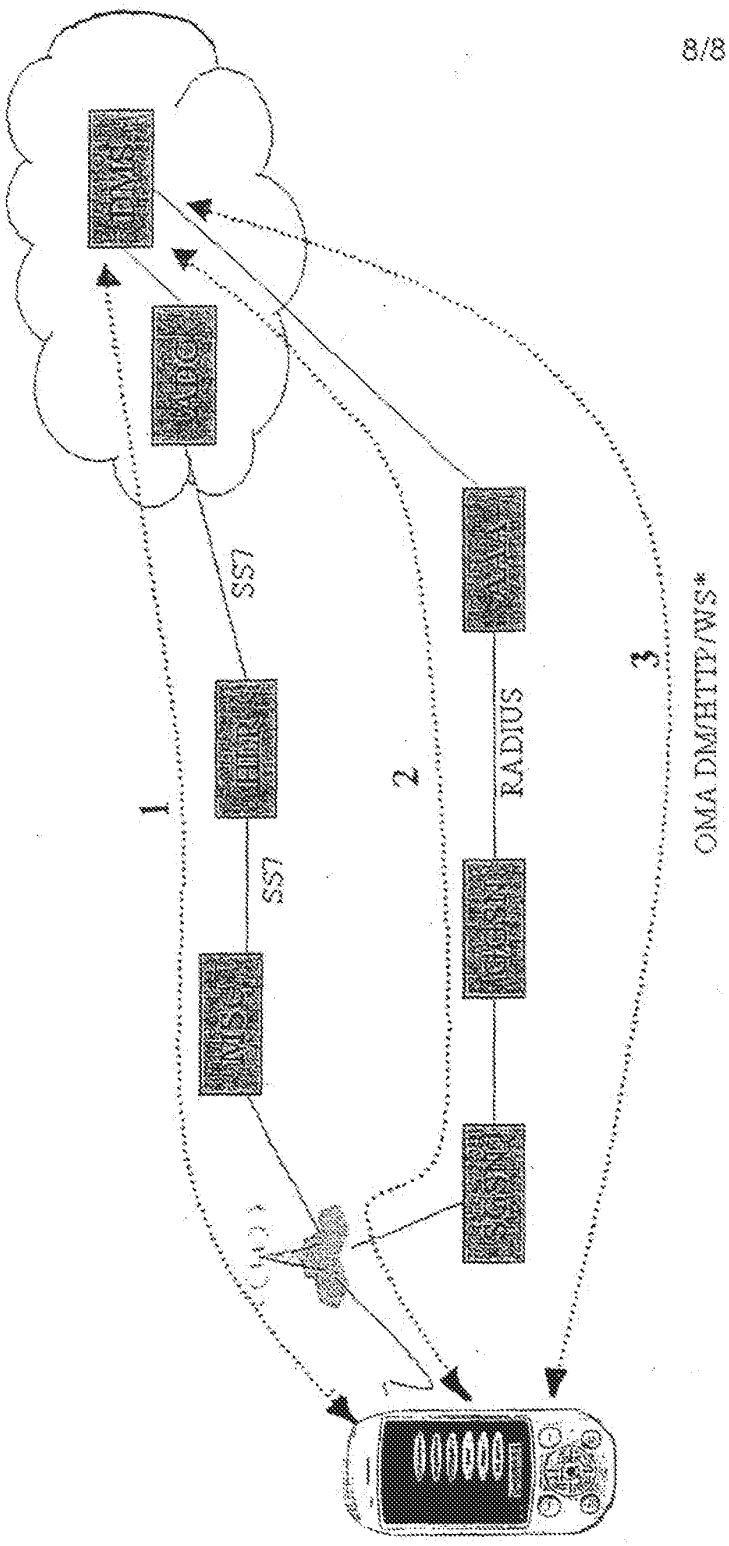


Fig. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/006776

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q7/38 H04L29/08 H04M3/42

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)
H04Q H04L H04M

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.
Y	EP 1 376 989 A (OPENWAVE SYSTEMS INC) 2 January 2004 (2004-01-02) abstract paragraphs [0060], [0069] - [0071]	1-40
Y	WO 02/091702 A (SIEMENS AKTIENGESELLSCHAFT; KUNZ, ALBRECHT; LEITGEB, MANFRED; SWETINA,) 14 November 2002 (2002-11-14) abstract page 6, line 18 - line 24 page 8, line 5 - line 25 page 9, line 21 - line 27 page 11, line 20 - line 35	1-3,7-9, 11-14, 17, 19-22, 26-28, 30-33, 36,38-40

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 October 2006	17/10/2006

Name and mailing address of the ISA/
European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer
Rüschmann, Frank

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DEVICE MANAGEMENT WORKING GROUP: "OMA Device Management Tree and Description OMA-TS-DM-TND-V1_2-20050615-C" OMA, 15 June 2005 (2005-06-15), pages 1-48, XP002360958 page 4, paragraph 4 page 5, paragraph 5 page 23, paragraph 8 - page 24, paragraph 8.2 page 25, paragraphs 9,9.1	4-6,10, 15,16, 18, 23-25, 29,34, 35,37, 39,40
A	EP 0 685 972 A (NOKIA MOBILE PHONES LTD; NOKIA CORPORATION) 6 December 1995 (1995-12-06) column 1, line 10 - line 27 column 8, line 7 - line 36 column 9, line 1 - line 36	1,8,9, 11,17, 19,20, 27,28, 30,36, 38-40
A	WO 00/67501 A (NOKIA MOBILE PHONES LTD; TERVO, VESA; MAEKELAE, SATU) 9 November 2000 (2000-11-09) page 13, line 3 - page 14, line 16 page 16, line 32 - page 17, line 34 page 26, line 21 - page 27, line 14	1,8,9, 11,17, 19,20, 27,28, 30,36, 38-40

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2006/006776

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1376989 A	02-01-2004	US 2004024867 A1	05-02-2004
WO 02091702 A	14-11-2002	EP 1386466 A1	04-02-2004
EP 0685972 A	06-12-1995	DE 69532597 D1	01-04-2004
		DE 69532597 T2	16-12-2004
		FI 942548 A	01-12-1995
WO 0067501 A	09-11-2000	AU 4407100 A	17-11-2000
		CN 1359599 A	17-07-2002
		EP 1175797 A1	30-01-2002
		FI 991000 A	31-10-2000
		JP 2002543720 T	17-12-2002

Form PCT/ISA/210 (patent family annex) (April 2005)

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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
12 January 2006 (12.01.2006)

(10) International Publication Number
WO 2006/004467 A1

(51) International Patent Classification[7]: H04Q 7/38, H04L 12/56

(21) International Application Number: PCT/SE2004/001087

(22) International Filing Date: 5 July 2004 (05.07.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SKOG, Robert** [SE/SE]; Gullvivegränd 7, S-165 76 Hässelby (SE). **PETERSSON, Justus** [SE/SE]; Sankt Paulsgatan 28B, S-118 48 Stockholm (SE).

(74) Agent: **DR LUDWIG BRANN PATENTBYRÅ AB**; P.O. Box 171 92, S-104 62 Stockholm (SE).

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

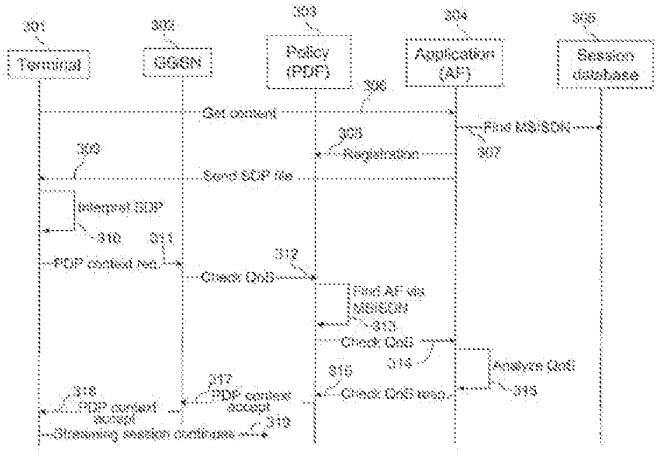
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU,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

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

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

(54) Title: BINDING MECHANISM FOR QUALITY OF SERVICE MANAGEMENT IN A COMMUNICATION NETWORK



(57) Abstract: The present invention relates to methods and arrangements for setting up a policy controlled bearer service for delivery of a service from an application function (304) to a mobile terminal (301). According to the present invention a terminal identity of the mobile terminal may be used to bind to applicable policy information when setting up the bearer service. Thus the present invention obviates the need to transmit specific binding information to the mobile terminal during application layer signaling for the purpose of policy controlled bearer service set-up. The terminal identity is registered (308) in a register of a policy decision function (303) along with policy identifying information. When a bearer service activation request is received from the mobile terminal (301) the request is mapped (313) to applicable policy information by means of the terminal identity and the matching registration in the register of the policy decision function (303).

WO 2006/004467 A1

BINDING MECHANISM FOR QUALITY OF SERVICE MANAGEMENT IN A COMMUNICATION NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to commonly-assigned co-pending international patent application No. PCT/SE04/_____, entitled "Devices and Methods for Push Message Initiated Service", filed on July 5, 2004; international patent application No. PCT/SE04/_____, entitled "Methods and Devices for Supplying Quality of Service Parameters in HTTP Message", filed on July 5, 2004; and international patent application No. PCT/SE04/_____, entitled "Methods and Devices for Changing Quality of Service", filed on July 5, 2004, the disclosures of which are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates to equipment and methods in mobile communication systems, and more particularly, to mechanisms for quality of service management of transmissions relating to a packet data service.

BACKGROUND

Communication networks for packet based communication of information in the form of data bits are well known to the person skilled in the art. The growing importance of mobile communication creates the demand to transfer data over wireless connections. The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that brings together a number of telecommunications standards bodies and was established to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support. This includes maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports including evolved radio access technologies (e.g. General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)).

One of the issues that the 3GPP is currently working on is a framework for providing end-to-end Quality of Service for services involving GPRS networks as described in the technical specification 3GPP TS 23.207 V6.2.0 (2004-03). This technical specification describes the use of a Policy Control mechanism in order to control and authorize the use of network resources prior to set-up of a service.

In the future it is assumed that packet switched services undergo Policy Control by means of a Policy Decision Function (PDF). The PDF is a logical element that is used as a logical policy decision element and enables coordination between events in the application layer and resource management in the IP bearer layer.

Policy Control was developed since it is considered important that network managers and service providers can to monitor, control, and enforce the use of network resources and services based on "policies" derived from certain criteria such as the identity/authority level of users and applications, traffic bandwidth requirements, security considerations, time of day/week etc. Because there are varying circumstances in which various entities are entitled to use the services they request, there is a need for rules, need for enforcement methods of these rules, and a need for a "judge" to decide when they apply. Accordingly, three major components of a policy system include policy rules, which are typically stored in a policy database, policy enforcement, which may be implemented at Policy Enforcement Points (PEP), and Policy Decision Points. The IETF has standardized a protocol for information exchange between PEPs and Policy Decision Points under the term Common Open Policy Service (COPS). In general, a policy may be regarded as a collection of rules that result in one or more actions when specific conditions exist.

Fig. 1 is a schematic block diagram that illustrates the different elements that are involved in the policy control mechanism developed by 3GPP. Fig. 1 illustrates an example where a service is set-up between a mobile User Equipment (UE) 1 and an Application Function (AF) of a service provider. The

UE includes an AF Client 3 which communicates with the AF 2 by means of AF session signaling 4 in order to initiate an application session. The set-up of the session and activation of the service require set-up of a bearer service to carry the data packets of the session. The session may include one or a plurality of different IP flows with specific requirements for bearer resources. The AF session signaling 4 may include information on Quality of Service (QoS) requirements which are translated into bearer QoS parameters by a translation/mapping function 5 in the UE. In order to activate the bearer service the UE sends a request for activation of a PDP context with the bearer QoS parameters that are determined by the translation/mapping function to a GGSN 6. The communication between the UE and the GGSN is in this example handled by means of UMTS BS Managers 7, 8 in the UE and the GGSN respectively. In this example the GGSN functions as a PEP and is provided with an IP BS Manager 9 which is involved in QoS management. The GGSN 6 interacts with a PDF 10, via a Go interface 11, in order to execute policy control. The PDF 10 makes policy decisions based on policy set-up information obtained from the AF 2 via a Gq interface 12. More detailed information regarding the elements illustrated in Fig. 1 and their function can be found in the above mentioned technical specification TS 23.207 V6.2.0.

When 3GPP specified the policy control mechanism an authorization token was also introduced in order to establish a binding mechanism for mapping PDP contexts and IP flows to policy information. The authorization token is generated by the PDF for a particular AF session on request from the AF. The authorization token includes a fully qualified domain name of the PDF and is unique across all PDP contexts associated with an APN (Access Point Name). The AF sends the authorization token to the UE in the AF session signalling. The UE should then include the applicable authorization token in any request to activate or modify a PDP context. The authorization token will then be used in the GGSN and PDF to map to the correct policy information.

The plan to introduce the authorization token and the associated handling of it when implementing policy control in 3G systems has a number of

disadvantages. One major disadvantage is that it requires modification of existing UEs in order to make them capable to handle authorization tokens. Another disadvantage is that the introduction of the authorization token requires new standardization for the RTSP (Real-Time Streaming Protocol), SIP (Session Initiation Protocol), and SDP (Session Description Protocol) and other protocols used in set-up and handling of application sessions.

SUMMARY OF THE INVENTION

An object of the present invention is to provide devices and methods for employing a simple binding mechanism when setting up a policy controlled bearer service for delivery of a service to a mobile terminal.

The above stated object is achieved by means of methods according to claim 1 and 10, and by means of a policy decision function according to claim 19.

The basic idea of the present invention is to use a terminal identity as binding information in order to bind a bearer service activation request to the applicable policy information and thereby obviate the need to transmit an authorization token to the terminal during bearer service activation.

According to a first aspect of the present invention a method for setting up a policy controlled bearer service for delivery of a service from an application function to a mobile terminal is provided. The method includes the steps of registering a terminal identity of the terminal associated with policy identifying information in a register of a policy decision function; receiving a bearer service activation request from the terminal, via a core network node, which bearer service activation request includes the terminal identity, such as MSISDN, IMEI , IMSI etc. and a set of requested QoS parameters for the bearer service; binding the bearer service activation request to the policy identifying information by means of the terminal identity to determine applicable policy information for the bearer service; performing a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and sending an accept message to the core network node