to initiate completion of the bearer service set-up if the policy check was successful.

According to a second aspect the present invention a method in a policy decision function for performing policy control on a bearer service for delivery of a service from an application function to a mobile terminal is provided. The method according to the second aspect of the invention comprises the steps of receiving a registration message, including a terminal identity and policy identifying information; registering the terminal identity associated with the policy identifying information in a register; receiving a bearer service activation request from the terminal, via a core network node, which bearer service activation request includes the terminal identity and a set of requested QoS parameters for the bearer service; binding the bearer service activation request to the policy identifying information in the policy decision function 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 to initiate completion of the bearer service set-up if the policy check was successful.

According to a third aspect of the present invention a policy decision function for performing policy control on a bearer service for delivery of a service from an application function to a mobile terminal is provided. The policy decision function includes a first interface for receiving a registration message, including a terminal identity and policy identifying information; a register for registering the terminal identity associated with the policy identifying information; a second interface for receiving a bearer service activation request from the terminal, via a core network node, which bearer service activation request includes the terminal identity and a set of requested QoS parameters for the bearer service; andprocessing means for binding the bearer service activation request to the policy identifying information in the policy decision function 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 for sending an accept message to the core network node to initiate completion of the bearer service set-up if the policy check was successful.

An advantage of the present invention is that it obviates the need to transmit an authorization token to the terminal for the purpose of setting up a policy controlled bearer service. This means that there is no impact on the terminals from a standard on the terminal.

Another advantage of the present invention is that by means of the present invention, no new standardization is required for 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.

A further advantage of the present invention is that the policy mechanism and QoS control mechanism of the invention are possible to implement in the mobile terminals that are available on the market today. Thus there is no need to modify the mobile terminals in order to implement the present invention.

Another advantage according to an embodiment of the present invention is that it allows for a service provider to upgrade the QoS parameters that a terminal requests for a bearer service if the requested QoS parameters do not fulfill the service providers QoS demand. This is possible since an embodiment of the present invention allows for the possibility to check if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the application function. If the predefined minimum QoS requirements are not fulfilled by the requested QoS parameters it is possible to determine modified QoS parameters for use when setting up the bearer service.

Further advantages and features of embodiments of the present invention will become apparent when reading the following detailed description in conjunction with the drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic block diagram illustrating the different elements that are involved in the policy control mechanism developed by 3GPP

Fig. 2 is a schematic block diagram illustrating the general network architecture of a mobile communication system in which the present invention may be used.

Fig. 3 is a schematic flow diagram illustrating an embodiment of a method according to the present invention.

Fig. 4 is a schematic flow diagram illustrating an alternative embodiment according to the present invention.

## DETAILED DESCRIPTION

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. In the drawings, like numbers refer to like elements.

The present invention is applicable to packet switched services in a mobile communication system. Such services include packet switched communication between a mobile client terminal of an end-user and an application server. The mobile communication system includes a radio

network such as for example a WCDMA, CDMA2000, Wireless LAN or GPRS network in which the mobile client terminal resides.

Fig. 2 is a schematic block diagram illustrating the general network architecture of a mobile communication system in which the present invention may be used. The mobile system 101 in fig. 1 comprises a mobile client terminal 102 which may communicate with a network node 106 of a service provider and thereby receive a service that is offered by the service provider. The communication between the client terminal 102 and the network node 106 is carried out via a radio network 103, a core network 104 and a service network 105. The radio network 103 may for instance be a UTRAN (UMTS Terrestrial Radio Access Network), the core network 104 may for instance be a UMTS Core Network and the service network may for instance be the Internet or a private IP network of a service provider. The network node 106 of the service provider may for instance be an application server.

Fig. 3 is a schematic flow diagram illustrating an embodiment of a method according to the present invention. The figure illustrates the interaction between a mobile terminal 301, a GGSN (Gateway GPRS Support Node) 302, a policy decision function (PDF) 303, an application function (AF) 304 and a session database 305 when setting up a policy controlled bearer service. Further network nodes may be involved in the process of setting up the bearer service but only the nodes that are of particular relevance to the present invention are illustrated in fig. 3 to simplify the description of the invention.

In fig. 3 it is assumed that a primary PDP context exists and that the terminal 301 asks the AF 304 for a streaming content, step 306. The AF is in this example a streaming server. The AF could also be for instance an MMS or Download server.

After receiving the request for a streaming content the AF 304 finds a terminal identity associated with the terminal 301. In this example the

terminal identity is an MSISDN (Mobile Identification Number) which is found by asking the session database 305 for a mapping between a terminal IP-address and MSISDN according to a method that is well known to the person skilled in the art, step 307. The AF then registers in the PDF 303 that it is interested in checking the QoS of the PDP context that is to be set up for delivery of the requested streaming content, step 308. The registration involves registering the MSISDN associated with policy identifying information in a register in the PDF. In this example the policy identifying information is an IP address of the AF so that the AF can be asked for applicable policy information. It is assumed that the address to the PDF is previously known to the AF. After the registration in the PDF, the AF sends an SDP-file to the terminal, step 309. The terminal then interprets the SDP-file and deduces QoS parameters to request for the bearer service to be set-up for delivery of the streaming content, step 310. The terminal then initiates a secondary PDP context by means of sending a activation request for a second PDP context, step 311. The activation request includes the QoS parameters that were deduced form the interpretation of the SDP-file. These QoS parameters will hereafter be denoted as requested QoS parameters. The steps 309, 310 and 311 are well known to the person skilled in the art and will therefore not be described in greater detail herein.

The GGSN 302 receives the PDP context activation request. The GGSN sends a request to the PDF to check the requested QoS parameters, step 312. The check request includes the MSISDN of the mobile terminal and the requested QoS parameters. It is assumed that the address of the PDF is known to the GGSN. When receiving the check request the PDF 303 finds the address of the AF 304 by mapping the MSISDN received in the check request to the register in which the AF's previous registration is stored, step 313. The PDF 303 then sends a check request to the AF 304 with the address that matches the MSISDN of the terminal in the register, step 314. The check request includes the MSISDN of the terminal and the requested QoS parameters. The AF 304 processes the QoS parameters and performs a policy check of the QoS parameters, step 315. The policy check may include checking that the QoS requirements does not succeed the limits of a subscription of the user of

the mobile terminal according to the principles described for the policy mechanism specified by 3GPP.

According to an embodiment of the present invention the policy check may also include a supplemental check that includes checking that the requested QoS parameters fulfil a set of predefined minimum QoS parameters which define the QoS that the service provide considers desired or needed for the bearer service. This supplemental check allows for the application function to initiate an upgrade of the QoS requirements if the requested QoS parameters do not achieve the QoS that the service provider considers desired or needed. The supplemental check and the mechanism for upgrading the requested QoS parameters will be described in further detail below.

After the AF 304 has checked the requested QoS parameters the AF sends an accept message or a modify message back to the PDF, step 316. If the policy check showed that the requested QoS parameters fulfilled the applicable policy, and selectively also the predefined minimum QoS parameters an accept message is sent. A modify message may be sent if the requested QoS parameters exceed the applicable policy and will in that case include an order to downgrade the requested QoS parameters. The order to downgrade the requested QoS parameters may be in the form of a set of downgraded QoS parameters to be used when setting up the bearer service. If the policy check includes checking that the requested QoS parameters match the predefined minimum QoS parameters a modify message may be sent if the requested QoS parameters are considered to result in a QoS that is poorer than what the service provider has defined as desired or needed. In that case the modify message may include an order to upgrade the requested QoS parameters. The order to upgrade the requested QoS parameters may be in the form of a set of upgraded QoS parameters to be used when setting up the bearer service.

After receiving the accept or modify message from the AF 304 the PDF 303 answers back to the GGSN. In this example the PDF sends a message

accepting the secondary PDP context to the GGSN, step 317. If the policy check resulted in a decision to modify the requested QoS parameters the message from the PDF 303 to the GGSN 302 may include modified QoS parameters to be used when setting up the secondary PDP context.

The set-up of the secondary PDP context is then completed by means of the PDP context set-up messages that are well known to a person skilled in the art. This includes that the GGSN answers back to the terminal via radio and core network nodes (not shown), step 318. When the PDP context is set-up the streaming session continues, step 319 and the streaming content may be delivered to the terminal over the secondary PDP context.

In fig. 3 it was illustrated that the policy check included that the PDF 303 asked the AF 304 to check the requested QoS parameters. It is however possible that this check is performed by the PDF. The AF may for instance send the applicable policy information and selectively also the set of predefined minimum QoS parameters to the PDF when it received the check request from the PDF. It is also possible that the applicable policy information was transferred to the PDF during the step 308 of registering the terminal identity in the PDF. The applicable policy information could then be stored in the register in the PDF along with the terminal identity.

In the above description of an embodiment of the invention it was mentioned that it was assumed that the AF and the GGSN was aware of the address of the PDF. This may for instance be the case if the network architecture was configured such that there is a preconfigured relationship between a single PDF and a number of GGSNs and a number of AFs. Each GGSN and each AF should in that case however be configured to only communicate with the single PDF for the purpose of achieving policy control.

A prerequisite of the binding mechanism that is provided by the present invention and which uses a terminal identity as binding information is that the mobile terminal requests activation of a single bearer service, such as a PDP context, at a time. The registration of the terminal identity in the PDF

should preferably be removed after the policy check is completed so that the terminal may request set-up of another bearer service and have a new request mapped correctly to applicable policy information.

The supplemental check described above to determine if the requested QoS requirements match the QoS that the service provider considers desired or needed for the bearer service is optional but may be very advantageous since it allows the service provider to control the QoS too a higher degree than provided by prior art solutions. The service provider may be interested in making sure that the terminal does not map a received SDP-file to QoS parameters that the service provider considers unsuitable for the bearer service since they result in poor QoS. Poor QoS may have a bad reflection on the service provider even if the poor QoS is a result of the implementation of the terminal. The supplemental check is here presented in combination with a token unaware terminal (i.e. a terminal that is not aware of an authorization token according to prior art), but the supplemental check may also be implemented in a system that makes use of an authorization token as binding mechanism instead of the terminal identity as described herein.

If it is of interest to perform the supplemental check the AF should be implemented with information that defines a set of minimum QoS parameters against which the requested QoS requirements may be checked. If the supplemental check results in a decision to upgrade the requested QoS parameters modified QoS parameters which correspond to an upgrade of the requested QoS parameters may be determined by the AF or the PDF. It is also necessary that the GGSN is implemented such that it is able to handle an upgrade of the requested QoS parameters. The upgrade scenario may require new signalling between the GGSN and other core network nodes and radio network nodes.

Fig. 4 is a schematic flow diagram that illustrates a scenario in which the requested QoS parameters are upgraded because the requested bandwidth was considered to low from the viewpoint of the service provider/AF. Fig. 4 illustrates, apart from the mobile terminal 301, the GGSN 302, the PDF 303

and the AF 304, also a radio network node 401, which e.g may be a Radio Network Controller (RNC) or a Base Station Controller (BSC), and a SGSN (Serving GPRS Support Node) 402. The session database 305 is not shown in fig. 4, but the AF 304 may have an interface to the session database for retrieving specific session information. The dashed box 403 surrounds the new signalling scheme, compared with what is supported by the current 3GPP standard and which is needed in order to handle an upgrade of the requested QoS parameters. The steps 411-424 illustrated in fig. 4 will now be described.

Step 411 The user has an interactive/browsing session established.

Step 412 The user clicks on an "rtsp-link".

Step 413 Streaming session establishment is performed.

Step 414 The AF (Application/Streaming server) registers the terminal identity in the PDF (this step corresponds to step 308 of fig. 3).

Step 415 The terminal requests activation of a secondary PDP context (this step corresponds to step 311 of fig. 3).

Step 416 The GGSN initiates a policy/QoS check with the PDF (this step corresponds to step 312 of fig. 3).

Step 417 The PDF checks that the needed resource reservation that is defined by the requested QoS parameters, is within the subscribed limits and issues a check request towards the AF (this step corresponds to step 314 of fig. 3).

Step 418 The AF sees that the bandwidth must be updated to ensure satisfactory end-user QoS during the service provisioning. Thus, it requests more bandwidth than the terminal initially requested (this step corresponds to step 316 of fig. 3).

Step 419 The PDF replies back to the GGSN. The GGSN discovers that the bandwidth parameter has been changed to a higher value than what requested by the terminal. Thus, the GGSN needs to request an update of the secondary PDP context.

Step 420 The requests a modification (bandwidth upgrade) of the terminal's requested secondary PDP Context by sending a PDP

Context update request message to the SGSN 402 which forwards the request to the radio network node 401.

Step 421 The radio network node 401 checks if it has enough resources to upgrade the bandwidth parameter. In this scenario it has enough resources and replies back to the SGSN (and the GGSN via the SGSN) with an acknowledgement. If the radio network node had not had enough resources, it is possible that the set-up of the service would be interrupted and that the requested service would be denied.

Step 422 The SGSN responds (possible in parallel with step 421) to the terminal's PDP context activation request with a different bandwidth parameter than the terminal initially requested.

Step 423 The terminal issues a "Play request".

Step 424 The application session starts.

The reason why a supplemental check as described above may be desired is that it is the terminal that translates or maps the application level QoS parameters to bearer service QoS parameters such as PDP context parameters. The implementation of the translation/mapping function in the terminal is vendor specific and may thus vary between different terminals. If the service provider is interested in delivering services with good quality irrespective of the terminal that requests the service the supplemental check may be desirable.

An example of application level QoS parameters are those defined for UMTS (Universal Mobile Telecommunication System). In UMTS QoS is defined with a set of attributes that specifies the UMTS bearer service. The UMTS QoS attributes are the following:

- Traffic class
- Maximum bit-rate
- Guaranteed bit-rate
- Delivery order
- Maximum SDU size
- SDU format information

- SDU error ratio
- Residual bit error ration
- Delivery of erroneous SDUs
- Transfer delay
- Traffic handling priority
- Allocation/Retention Priority
- Source statistics descriptor
- Signaling Indication

These attributes can be mapped to the pre-defined UMTS QoS classes: Conversational class, Streaming class, Interactive class and Background class. More detailed information about UMTS QoS can be found in the technical specifications 3GPP TS 23.107 V6.1.0 (2004-03) and 3GPP TS 23.207 V6.2.0 (2004-03).

The QoS classes can be negotiated and managed by using PDP context management. Application level QoS requirements are mapped to PDP context parameters in the mobile client terminal. In prior art solutions pre-configurations of PDP contexts are made in the client terminal such that when a packet switched application starts and connects to the network a matching pre-configured PDP context is activated. This PDP context has a selected QoS class that should match the desired QoS requirements of the application. If for instance the application is a WAP browser or MMS client the QoS class of the activated PDP context is usually the Interactive class.

Thus in the prior art solutions the selection of QoS parameters for the bearer service that is set up for delivery of the service in the example depends on the terminal vendor's configuration of the mobile client terminal. The service provider cannot influence the selection of the QoS parameters. As mentioned above this is in many instances problematic, especially from the viewpoint of the service provider, but also from a user perspective, when it results in set-up of a bearer service with a QoS that is not appropriate for the delivery of the service. The service provider is usually interested in being able to ensure that the offered service is delivered with a certain minimum quality. If the quality of service is bad this may have a negative impact on the service

provider's reputation even if the bad quality is caused by a network operator or terminal vendor. The user of the service will become annoyed if the QoS is bad and will probably blame the service provider for the bad quality. It is also possible that a user with one terminal gets unacceptably bad QoS when receiving a particular service content while another user, with a terminal from another vendor, gets acceptable QoS when receiving the same service content.

However, as shown above, the embodiment of the present invention that includes a supplemental check, in which the service provider can control the requested QoS parameters and also modify them if is considered necessary, makes it possible to overcome many of the disadvantages that may arise when the terminal translates/maps application lever QoS requirements into bearer service QoS parameters.

In the drawings and specification, there have been disclosed typical preferred embodiments of the invention and, although specific terms are employed, they are used in a generic and descriptive sense only and not for purposes of limitation, the scope of the invention being set forth in the following claims.

# CLAIMS

1. A method for setting up a policy controlled bearer service for delivery of a service from an application function (304) to a mobile terminal (301), which method comprises

registering (308) a terminal identity of the terminal (301) associated with policy identifying information in a register of a policy decision function (303);

receiving (312) a bearer service activation request from the terminal, via a core network node (302), which bearer service activation request includes the terminal identity and a set of requested QoS parameters for the bearer service;

binding (313) 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 (314, 315, 316) a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and

sending (317, 318) an accept message to the core network node to initiate completion of the bearer service set-up if the policy check was successful.

2. The method according to claim 1, wherein said terminal identity is a Mobile Identification Number, MSISDN, an International Mobile Subscriber Identity, IMSI, or an International Mobile Equipment Identity, IMEI, associated with the terminal (301).

3. The method according to claim 1 or 2, wherein said policy identifying information includes an address of the application function (304) and wherein the step (313) of binding the bearer service activation request to the policy identifying information includes requesting (314) the applicable policy information from the application function (304) identified by the application address in the policy identifying information.

4. The method according to claim 1 or 2, wherein said policy identifying information includes the applicable policy information for the bearer service to be set up.

5. The method according to any of claims 1-4, wherein said step of performing a policy check includes checking (315) if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the application function (304).

6. The method according to claim 5, wherein the method includes a further step of determining a set of modified QoS parameters that match the set of predefined minimum QoS requirements if the requested QoS parameters do not fulfill the set of predefined minimum QoS requirements, and a further step of sending (316, 317) the set of modified QoS parameters to the core network node (302) for use when setting up the bearer service.

7. The method according to any of claims 1-6, wherein the core network node (302) is a Gateway GPRS Support Node, GGSN.

8. The method according to any of claims 1-7, wherein the method includes a further step of removing the registration of the terminal identity and the policy identifying information from the register of the policy decision function (303) after the step (314, 315, 316) of performing the policy check.

9. The method according to any of claims 1-8, wherein said bearer service is a Packet Data Protocol, PDP, context.

10. A method in a policy decision function (303) for performing policy control on a bearer service for delivery of a service from an application function (304) to a mobile terminal (301), which method comprises the steps of

receiving (308) a registration message, including a terminal identity and policy identifying information;

registering the terminal identity associated with the policy identifying information in a register;

receiving (312) a bearer service activation request from the terminal (301), via a core network node (302), which bearer service activation request

includes the terminal identity and a set of requested QoS parameters for the bearer service;

binding (313) the bearer service activation request to the policy identifying information in the register by means of the terminal identity to determine applicable policy information for the bearer service;

performing (314) a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and

sending (317) an accept message to the core network node (302) to initiate completion of the bearer service set-up if the policy check was successful.

11. The method according to claim 10, wherein said terminal identity is a Mobile Identification Number, MSISDN, an International Mobile Subscriber Identity, IMSI, or an International Mobile Equipment Identity, IMEI, associated with the terminal (301).

12. The method according to claim 10 or 11, wherein said policy identifying information includes an address of the application function (304) and wherein the step (313) of binding the bearer service activation request to the policy identifying information includes requesting (314) the applicable policy information from the application function (304) identified by the application address in the policy identifying information.

13. The method according to claim 10 or 11, wherein said policy identifying information includes the applicable policy information for the bearer service to be set up.

14. The method according to any of claims 10-13, wherein said step of performing a policy check includes checking if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the application function (304).

15. The method according to claim 14, wherein the method includes a further step of determining a set of modified QoS parameters that match the set of predefined minimum QoS requirements if the requested QoS

parameters do not fulfill the set of predefined minimum QoS requirements, and a further step of sending (317) the set of modified QoS parameters to the core network node (302) for use when setting up the bearer service.

16. The method according to any of claims 10-15, wherein the core network node (302) is a Gateway GPRS Support Node, GGSN.

17. The method according to any of claims 10-16, wherein the method includes a further step of removing the registration of the terminal identity and the policy identifying information from the register after the step of performing the policy check.

18. The method according to any of claims 10-17, wherein said bearer service is a Packet Data Protocol, PDP, context.

19. A policy decision function (303) for performing policy control on a bearer service for delivery of a service from an application function (304) to a mobile terminal (301), which policy decision function includes

a first interface for receiving (308) a registration message, including a terminal identity and policy identifying information;

a register for registering the terminal identity associated with the policy identifying information;

a second interface for receiving (312) a bearer service activation request from the terminal, via a core network node (302), which bearer service activation request includes the terminal identity and a set of requested QoS parameters for the bearer service; and

processing means for

binding (313) the bearer service activation request to the policy identifying information in the policy decision function by means of the terminal identity to determine applicable policy information for the bearer service;

performing (314) a policy check by means of checking if the requested QoS parameters fulfill said applicable policy information; and

sending (317) an accept message to the core network node (302) to initiate completion of the bearer service set-up if the policy check was successful.

20. The policy decision function (303) according to claim 19, wherein said terminal identity is a Mobile Identification Number, MSISDN, an International Mobile Subscriber Identity, IMSI, or an International Mobile Equipment Identity, IMEI, associated with the terminal (301).

21. The policy decision function (303) according to claim 19 or 20, wherein said policy identifying information includes an address of the application function (304) and wherein the processing means are arranged to request the applicable policy information from the application function (304) identified by the application address in the policy identifying information.

22. The policy decision function (303) according to claim 19 or 20, wherein said policy identifying information includes the applicable policy information for the bearer service to be set up.

23. The policy decision function (303) according to any of claims 19-22, the processing means are further arranged to check if the requested QoS parameters fulfill a set of predefined minimum QoS requirements provided by the application function (304).

24. The policy decision function (303) according to claim 23, wherein the processing means are further arranged to determine a set of modified QoS parameters that match the set of predefined minimum QoS requirements if the requested QoS parameters do not fulfill the set of predefined minimum QoS requirements, and to send (317) the set of modified QoS parameters to the core network node for use when setting up the bearer service.

25. The policy decision function (303) according to any of claims 19-24, wherein said processing means are arranged to remove the registration of the

terminal identity and the policy identifying information from the register after the processing means has completed the policy check.

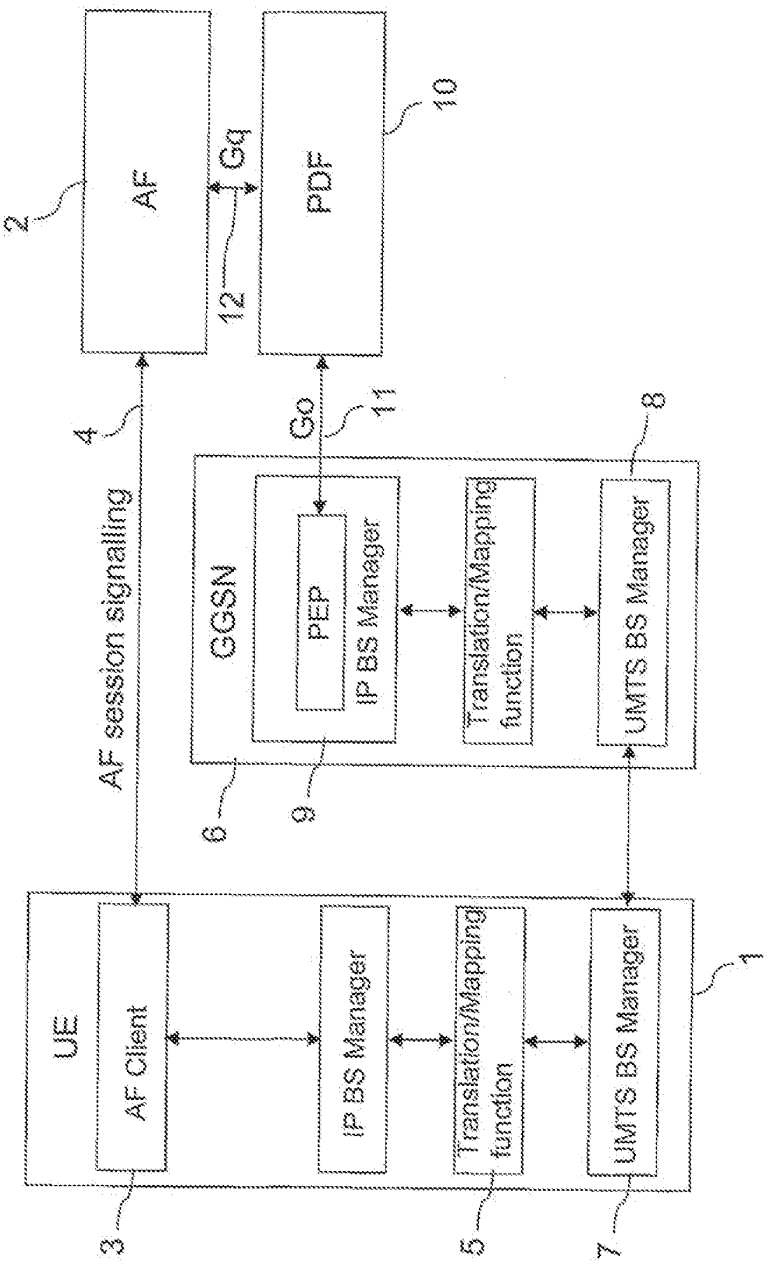

UE
AF Client
IP BS Manager
Translation/Mapping function
UMTS BS Manager
1
3
5
7
AF session signalling
4
AF
2
Gq
12
PDF
10
Go
11
GGSN
PEP
IP BS Manager
Translation/Mapping function
UMTS BS Manager
8
6
9

Fig. 1

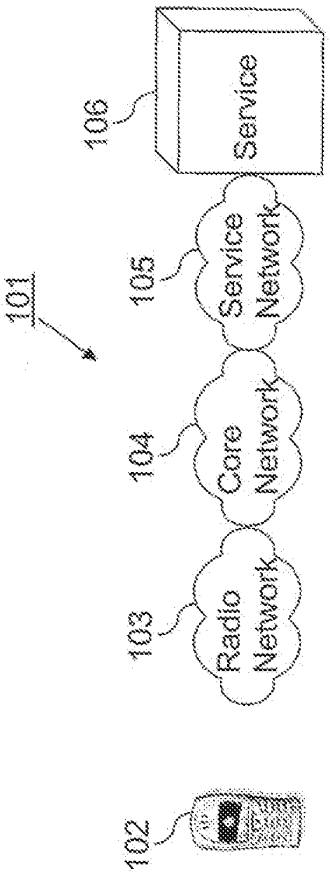

101
102
103
Radio Network
104
Core Network
105
Service Network
106
Service

Fig. 2

3/4

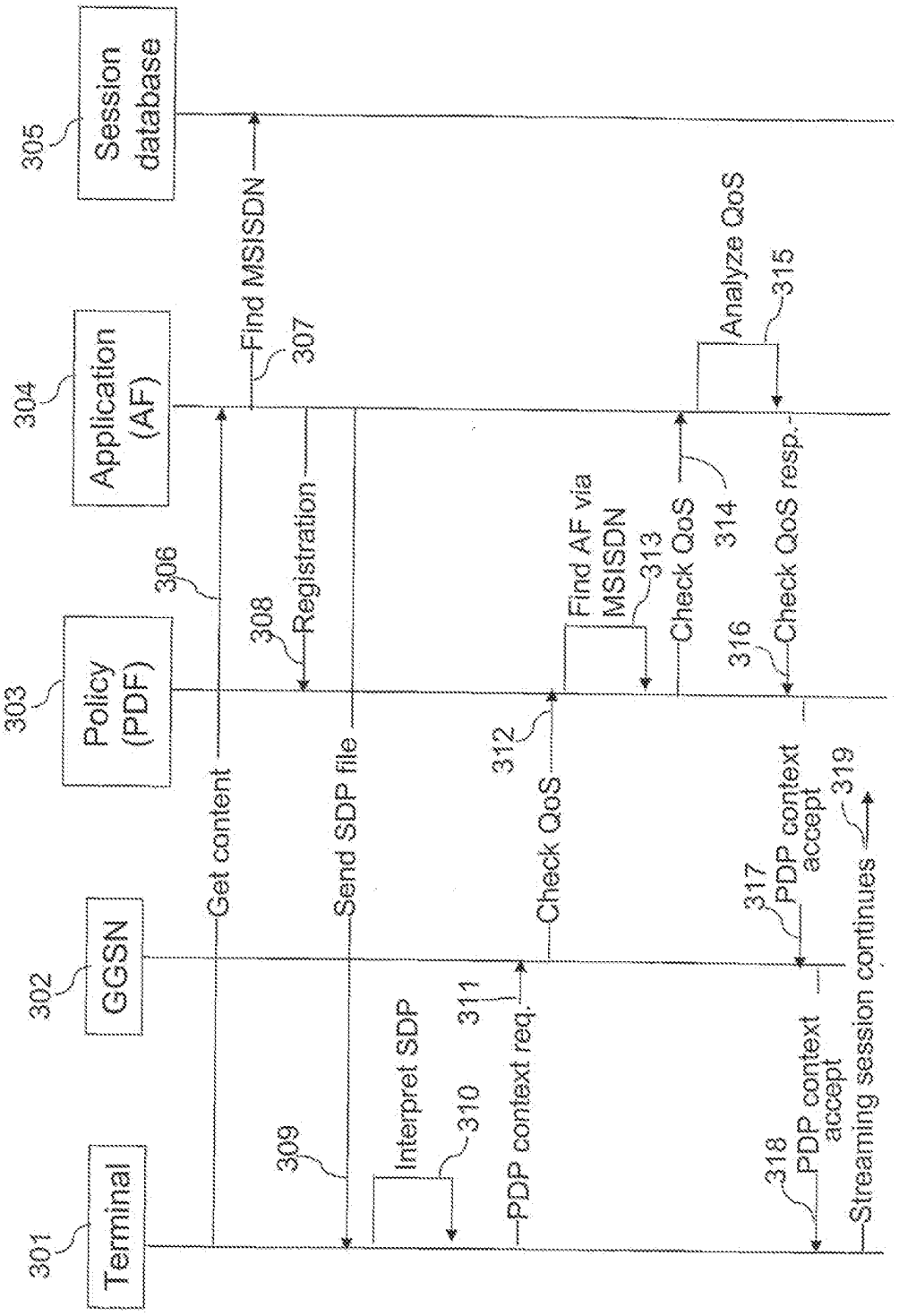

Terminal
301
GGSN
302
Policy (PDF)
303
Application (AF)
304
Session database
305
Get content
306
Find MSISDN
307
Registration
308
Send SDP file
309
Interpret SDP
310
PDP context req.
311
Check QoS
312
Find AF via MSISDN
313
Check QoS
314
Analyze QoS
315
Check QoS resp.
316
PDP context accept
317
PDP context accept
318
Streaming session continues
319

Fig. 3

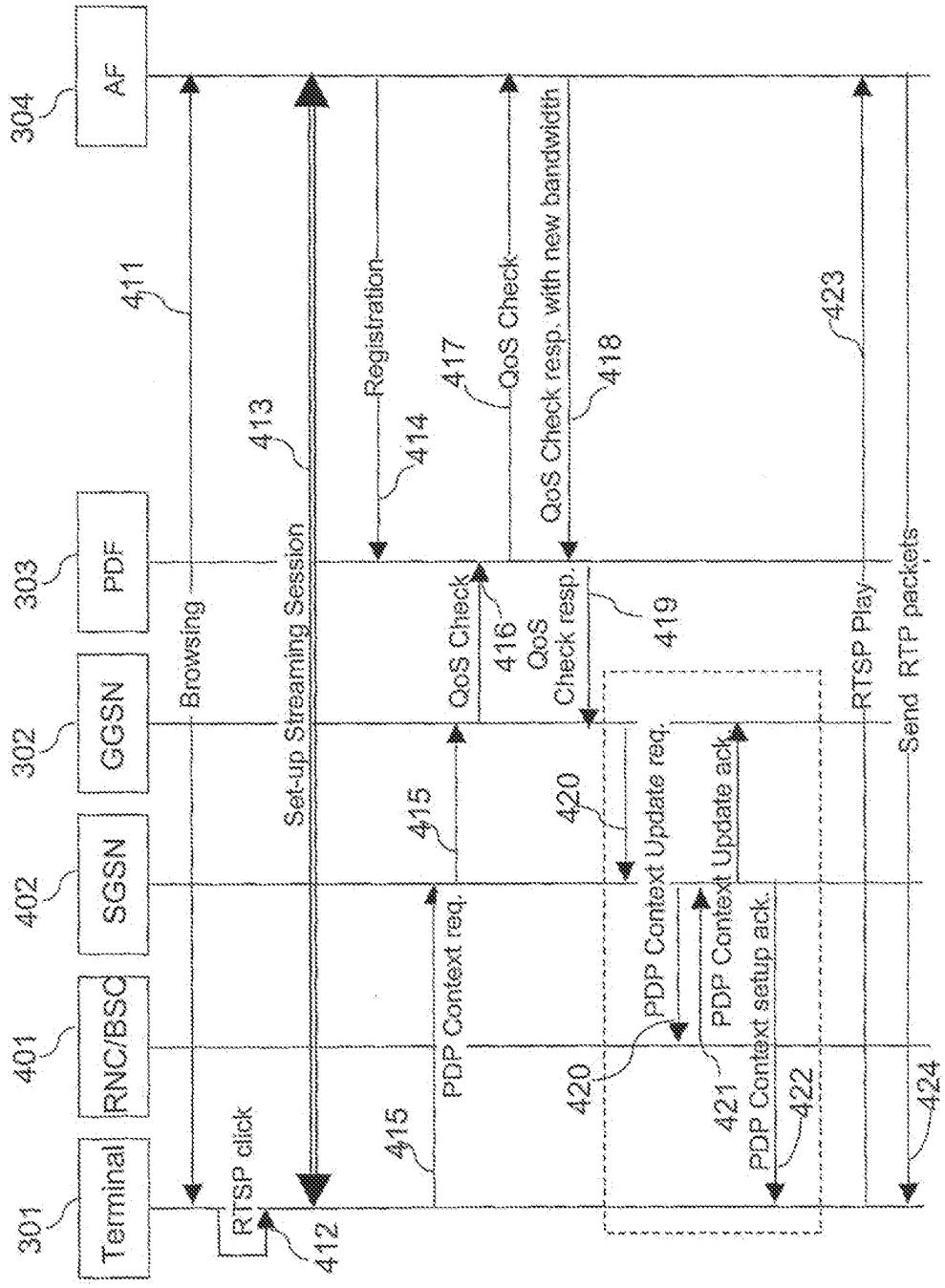

301
Terminal
401
RNC/BSC
402
SGSN
302
GGSN
303
PDF
304
AF
RTSP click
412
Browsing
411
Set-up Streaming Session
413
Registration
414
PDP Context req.
415
QoS Check
416
QoS Check resp.
417
QoS Check resp. with new bandwidth
418
419
PDP Context Update req.
420
PDP Context Update ack.
421
PDP Context setup ack.
422
RTSP Play
423
Send RTP packets
424

Fig. 4

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 2004/001087

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04L 12/56
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, H04Q

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | ETSI TS 123 207 V5.9.0 (2004-03) Digital cellulär telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); End-to-end Quality of Service (QoS) concept and architecture (3GPP TS 23.207 version 5.9.0 Release 5). See chapter 6 -- | 1-25 |
| A | WO 03049348 A2 (NOKIA INC), 12 June 2003 (12.06.2003), claims 1,8,9, abstract -- | 1-25 |

☐ 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 |
|---|---|
| 18 February 2005 | 24 -02- 2005 |
| Name and mailing address of the ISA/<br>Swedish Patent Office<br>Box 5055, S-102 42 STOCKHOLM<br>Facsimile No. +46 8 666 02 86 | Authorized officer<br>Lisbeth Andersson /LR<br>Telephone No. +46 8 782 25 00 |

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| WO | 03049348 | A2 | 12/06/2003 | AU | 2002353271 | A | 00/00/0000 |
| | | | | US | 6661780 | B | 09/12/2003 |
| | | | | US | 20030108015 | A | 12/06/2003 |

**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 12/00 — A2

(11) International Publication Number: **WO 99/65185**

(43) International Publication Date: 16 December 1999 (16.12.99)

(21) International Application Number: PCT/GB99/01773

(22) International Filing Date: 4 June 1999 (04.06.99)

(30) Priority Data:

| | | |
|---|---|---|
| 9812161.9 | 5 June 1998 (05.06.98) | GB |
| 98309609.0 | 24 November 1998 (24.11.98) | EP |
| 9825723.1 | 24 November 1998 (24.11.98) | GB |
| 9902052.1 | 29 January 1999 (29.01.99) | GB |
| 9902648.6 | 5 February 1999 (05.02.99) | GB |

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BRISCOE, Robert, John [GB/GB]; Home Farm, Parham, Woodbridge, Suffolk IP13 9NW (GB). RIZZO, Michael [MT/GB]; 12 Dewar Lane, Kesgrave, Ipswich, Suffolk IP5 2GJ (GB).

(74) Agent: EVERSHED, Michael; BT Group Legal Services, Intellectual Property Dept., 8th floor, Holborn Centre, 120 Holborn, London EC1N 2TE (GB).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**

*Without international search report and to be republished upon receipt of that report.*

(54) Title: COMMUNICATIONS NETWORK

(57) Abstract

In a communications network, loading of network resources is detected locally at a customer terminal, and a tariff for network usage is varied automatically depending on the usage.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | ML | Mali | TR | Turkey |
| BG | Bulgaria | HU | Hungary | MN | Mongolia | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MR | Mauritania | UA | Ukraine |
| BR | Brazil | IL | Israel | MW | Malawi | UG | Uganda |
| BY | Belarus | IS | Iceland | MX | Mexico | US | United States of America |
| CA | Canada | IT | Italy | NE | Niger | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NL | Netherlands | VN | Viet Nam |
| CG | Congo | KE | Kenya | NO | Norway | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NZ | New Zealand | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | PL | Poland | | |
| CM | Cameroon | KR | Republic of Korea | PT | Portugal | | |
| CN | China | KZ | Kazakstan | RO | Romania | | |
| CU | Cuba | LC | Saint Lucia | RU | Russian Federation | | |
| CZ | Czech Republic | LI | Liechtenstein | SD | Sudan | | |
| DE | Germany | LK | Sri Lanka | SE | Sweden | | |
| DK | Denmark | LR | Liberia | SG | Singapore | | |
| EE | Estonia | | | | | | |

# Communications Network

## BACKGROUND TO THE INVENTION

The present invention relates to a communications network, and in particular to charging mechanisms in such a network. It includes aspects of the inventions disclosed and claimed in the present applicant's co-pending British patent application no. 9812161.9 filed 5 June 1998 (applicant's ref: A25547) and the contents of that earlier application are incorporated herein by reference.

In conventional communications networks, such as national PSTNs (public switched telephone networks), a significant proportion of the network resources are devoted to metering and billing network usage. Studies have estimated these resources as consuming as much as 6% of the revenue of a telecommunications company. The Internet, by contrast, does not in general incorporate metering and billing mechanisms for individual customers. The absence of the network infrastructure required to support metering and billing reduces the operational costs of the Internet compared to conventional telephony networks, and has facilitated the rapid expansion of the Internet. However, the absence of appropriate billing mechanisms has significant disadvantages in terms of the characteristics of the traffic carried by the Internet: it encourages profligate use of network resources, and diminishes the incentive for investment in network infrastructure to support new applications requiring, e.g., guaranteed quality of service (QoS).

## SUMMARY OF THE INVENTION

According to a first aspect of the present invention, there is provided a method of operating a communications network, including automatically varying, depending on network loading as detected at a customer terminal, a tariff for network usage by the customer terminal.

In this document references to varying a tariff encompass changing a price, e.g. as a function of a congestion parameter. The structure of the tariff may be unchanged.

The present invention provides an approach to charging for network usage which involves little or no network overheads, and which moreover is able to reflect local variations in network loading. This is achieved by detecting a measure of

network loading at the customer terminal. This measure will reflect those resources being used by the customer terminal at a particular time. For example, in a federated data network comprising a number of sub-domains, such as the Internet, a customer terminal in one subdomain may attempt to access a server in another subdomain at a time when there is overloading of a router somewhere in the path from the customer terminal to the server. Then, even if average loading of the network as a whole is low, the loading as perceived by the customer terminal is high, and a tariff for use of the network by the customer terminal is increased to reflect the scarcity of the relevant network resources. Similarly other terminals attempting to access data via the same router will also perceive the network loading as being high, and will also have their tariffs increased accordingly. With an appropriately steep rise in tariff, at least some customer terminals will then choose to abandon or defer their attempts to use the network resource in question, thereby relieving the loading of the router.

This aspect of the invention may be used in systems in which the end user is merely informed of the price and accounting and billing is carried out by the network provider, also in systems where the end user measures their usage and supplies this information to the network provider, and also in systems where the end user both measures their usage and calculates the payment due to the network provider.

The method may include detecting at the customer terminal a network performance parameter which depends on network loading, and varying the tariff depending on the network performance parameter. When the network is a packet network, then the network performance parameter may be the number of packets lost in transmission between a data source and the customer terminal. This approach has the advantage that it is suitable for implementation using existing congestion control mechanisms in packet networks. For example, in the Internet, routers respond to congestion by dropping packets, and a customer terminal using TCP (Transport Control Protocol) detects packet loss and controls a congestion window at the terminal accordingly. The present invention may use the detected packet loss to trigger an increase in the tariff applicable to the terminal. This may be accompanied by the signalling of congestion by the receiving terminal to the data source.

In an alternative and preferred approach, when congestion is detected within the network an explicit congestion signal may be generated and transmitted to the customer terminal, and the receipt of the explicit congestion signal at the customer

terminal may then trigger the increase in the tariff. This approach has the advantage that an appropriate congestion signal may be generated in advance of significant degradation in network performance occurring, making it easier to maintain a required quality of service. Preferably the explicit congestion signal is carried with a data packet on the communications network. Preferably a router in the network writes an explicit congestion signal in a packet when congestion is detected at the router.

As a further alternative, the congestion notification signal may be a source quench signal generated at the router and transmitted back to the data source.

Preferably there is a non-linear relationship between the increase in tariff and the detected network loading. Preferably the method includes making a first relatively smaller increase in the tariff when congestion is first detected, and making at least one further, relatively larger increase, if the congestion persists. This behaviour may be pre-programmed into the tariff algorithm. In this way oscillatory behaviour of the network can be avoided, while ensuring that a sufficient increase is made to have a desired impact on the demand for network resources.

Preferably the method includes programming a decision agent at the customer terminal with user-determined price criteria, and comparing a price calculated using the tariff with the said price criteria. For example, the decision agent might be programmed to proceed with data communications as long as a per-packet charge is zero or is less than a predetermined threshold. Then if congestion causes the charge to rise above that threshold, the data communication is interrupted and the decision agent modifies the operation of the customer terminal. For example the decision agent may slow down communications once the cost threshold is exceeded. The user may then choose to continue with the communication, or may elect to abandon the attempt to access data from a particular source. The decision agent may be programmed with rules which relate to an overall price for multiple simultaneous transmissions and which accord different weights to different respective applications.

Preferably the method includes distributing a tariff algorithm via the communications network to a plurality of terminals and calculating at each terminal using the tariff a charge for network usage by the terminal. In this case preferably the method includes steps, carried out by a network operator, of intermittently

sampling traffic between a customer terminal and the network, and as part of the sampling recording network loading affecting the customer terminal;

for the sampled traffic comparing a charge calculated by the customer terminal and an expected charge and detecting thereby any discrepancy.

The step of recording network loading may involve, for example, recording packet drops, or explicit congestion notification (ECN) bits or source quench messages.

The invention also encompasses a network operating by a method in accordance with the first aspect of the invention, and customer terminals, network routers and other network nodes for use in such a network.

## DESCRIPTION OF DRAWINGS

Systems embodying the present invention will now be described in further detail, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic showing a network embodying the invention;

Figures 2a and 2b are graphs showing tariff functions;

Figure 3 shows the format of a differential service byte;

Figure 4 is a schematic showing the component objects of a charging architecture for use with the network of Figure 1;

Figure 5 shows data passed between the accounting objects of Figure 4;

Figure 6 is a schematic showing protocol stacks on a customer terminal and in the network domain;

Figure 7 is a graph showing the variation of tariff with time;

Figures 8a to 8e are class diagrams for software implementing accounting and measurement objects;

Figure 9 is a diagram showing a graphic user interface (GUI) for use with the objects of figures 8a to 8e;

Figure 10 is a class diagram for software implementing tariff objects; and

Figure 11 is a diagram showing an alternative embodiment.

## DESCRIPTION OF EXAMPLES

As shown in Figure 1, a communications network 1 includes a number of network sub-domains 2A-C. The network sub-domains may be under the control of different operators who may not trust each other. The network subdomains are interconnected by gateway routers 3, 4. In the present example the communications network is the Internet and supports both unicast and multicast Internet Protocol (IP) and associated protocols. A customer terminal 5 is connected via a public switched telephony network (PSTN) 6 and an access router 7 to a subdomain 2A. A single blocking test is applied to traffic at this point of access. The gateway routers 3,4, and access router 7 may be commercially available devices such as CISCO series 7500 routers and CISCO series AS5800 universal access server respectively. Other customer terminals are connected to the network, including a Java-enabled mobile terminal 8 and a data server 9. The customer terminal 5 may be connected via a LAN to an accounting server. The accounting server may include an accounting object as described below that receives measurement data from the customer terminal.

In addition to the local tariff variation mechanism that is described below, the network also uses network-based control of a number of tariff bands. A network management platform 10 is connected to each subdomain. Each network management platform may comprise, for example, a computing system comprising a SPARC workstation running UNIX (Solaris) together with network management applications. The network management platform 10 hosts management entities and tariff entities. The network management platform communicates with agents 100 in managed devices connected to the respective subdomain, for example using SNMP (simple network management protocol). The management platforms monitors the overall loading of network resources in the respective subdomains, and, as will be further described below, adjust the tariffs for network use accordingly. The Net management platform (NMP) instructs the agent to monitor the device and report aggregated results at regular intervals back to the NMP, so the NMP can monitor the combination of all reports.

Tariff data is communicated to peer tariff entities in other subdomains and also to the customer terminals. The tariff data is multicast using, for example Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM) dense mode. The tariff data channels are announced and monitored

using protocols based on SDP (Session Description Protocol), SAP (Session Announcement Protocol) Charging is carried out on a "pay and display" model. Each customer terminal monitors its own network usage, for example by counting the number of packets it sends or receives across the network interface and the quantity of data (in bytes) in those packets. It calculates, using a tariff received via the network, the payment due to the network operator, and makes a corresponding payment into an account at the network operator. The network operator polices the use made by customers of the terminal by intermittently sampling traffic to or from a particular customer and comparing the use made and the use paid for.

The tariffs supplied to the customer terminals are divided into bands of different volatilities. The tariffs are varied under the control of the network operators to reflect the overall loading of the network. That is to say, if network loading becomes high, then the tariffs may be increased to reflect the scarcity of network resources.

A service provider may offer different products defined by different service level agreements, and/or by different price volatilities. For example product A might offer best-effort service at a fixed price while another product B might offer best-effort service at a variable price. A service provider may adjust product prices on the basis of the following parameters: the price the service provider pays to its wholesale provider: competitors' prices; current resource utilisation; relevant demand for different products. In response to changes in these parameters, tariff adjustments may be effected in one of three ways. Firstly, a tariff may adjust prices on the basis of local observations of network loading, without necessitating explicit communication from the provider. This approach, which is described in further detail below, needs to be built into the tariff at the outset, and is limited to those price variations which are dependent exclusively on local observations. Secondly, the provider may tune a tariff by adjusting some of its parameters. This kind of adjustment is required when the decision is dependent on parameters which cannot be observed directly by the customer, e.g., variation in the wholesale price of network resources. Thirdly, the provider may completely replace a tariff. This is required when the existing tariff cannot accommodate the changes that are required.

The first of the tariff changes described above is necessarily carried out automatically. The second type of change may be performed manually, or by an

agent that issues adjustments automatically in response to observations made by the service provider system. The third type of change is likely to be performed manually, as replacement of a new tariff will in general require an element of design requiring human input. However, it is possible that an agent might be employed to automatically switch tariffs for a product on the basis of a set of specified rules.

This section describes a prototype that we implemented to demonstrate the tariff subsystem outlined above. Features of the design include:

* using mobile code to represent tariffs and associated user interface components;
* use of a repeated multicast announcement protocol to communicate tariffs and tariff adjustments efficiently;
* using dynamic class loading and reflection in order to receive and tune tariffs.

The prototype consists of a library of general-purpose Java classes and two specific applications, namely:

* a provider system which allows the provider to introduce, replace, and tune tariffs for a number of products;
* a customer system that enables customer to keep track of the charges being applied for the products they are using.

The provider system services multiple instances of the customer system running on different hosts in a multicast-enabled network. A multicast announcement protocol is used to communicate tariff changes from the provider system to customer systems.

In order to maximise flexibility with respect to the definition of tariffs, we chose to represent tariffs using Java classes. This technique is also used to supply user interface components to customers to support visualisation of the behaviour of a tariff.

The `Tariff` interface acts as the base class for all tariffs. This defines a single operation get `GUI()` which returns as a Java SWING component that can be incorporated into the customer's GUI (graphical user interface). This GUI component enables the customer to visualise the behaviour of the tariff using techniques appropriate to the tariff.

Subclasses of the `Tariff` interface establish a set of tariff types, each of which is associated with a different set of measurement and input parameters. These parameters are identified by listing them in the signature of the `getCharge ()` method. For example, the interface `RSVPTariff` defines `getCharge ()` as

receiving n RSVP TSPEC, allowing for the definition of tariffs that compute price on the basis of the characteristics of an RSVP reservation. On the other hand, the interface PacketCountTariff defines getCharge () as receiving measurements of packets in, packets out, and current congestion (typically measured as a function of packet drop), allowing for the definition of tariffs that are dependent on packet counts and sensitive to congestion. Other tariffs may be added as new forms of usage-measurement emerge.

Tariffs are defined by providing implementations of the various tariff interfaces described above. For example, the tariff PacketCountLinear implements PacketCountTariff to compute charges in proportion to packet counts. Another tariff CongestionSensitiveLinear works on a similar basis, but adds a penalty charge if the customer does not stay within a specified traffic limit in the presence of congestion.

In addition to the tariff interface implementation, a tariff may make use of other 'helper' classes to assist in its operation, as well as one or more user interface component classes for customer visualisation purposes. A provider-side user interface may also be required in order to enable the provider to make tariff adjustments.

A complete tariff description consists of a set of Java classes, some of which are destined for the customer system and others which are intended for use by the provider system. The customer-side classes are bundled into a Java archive (JAR) file to facilitate processing by the provider system.

In order to deploy a new tariff, the provider system first loads the tariff classes which it requires into its execution environment. It then loads the customer-side bundle, serialises it, signs it with a private key, and uses an announcement protocol to distribute it to customer systems. The use of a signature makes it possible for customers to verify that received tariffs are authentic.

Upon receiving the bundle, each customer system verifies the signature (using the public key matching the provider's private key), and at the activation time specified in the announcement protocol headers which may be significantly later, e.g. hours or days, unpacks the bundle, and loads the classes into its execution environment using a purpose-built dynamic class loader. An instance of the received tariff class is created and installed in place of the previous tariff. If the tariff has a

user interface component (obtained by calling the tariff object's `getGUI()` method), then it replaces the user interface of the previous tariff. The change in user interface serves to notify the user that the tariff has changed.

Tariff adjustment involves the remote invocation of an operation which is specific to the tariff currently in force. This means that a customer system cannot know the signature of this operation in advance of receiving the tariff i.e. the operation will not be listed in any of the tariff interfaces known to the customer system.

In order to get around this problem, use is made of the "reflection" feature supported by Java. In order to disseminate a tariff adjustment, the provider creates an instance of an `Invocation` object, which stores the name of the operation to be called, together with the parameters that are to be supplied to it. This object is then serialised, signed, and announced using the announcement protocol. When an adjustment is receive and verified by a customer system, the `Invocation` object is de-serialised and applied to the current tariff by using reflection to invoke the described operation.

In order to simplify the announcement protocol, adjustments are required to be idempotent and complete. Idempotency guarantees that a tariff will not be adversely affected if an adjustment is applied more than once. Completeness implies that an adjustment determines the entire parameter set of a tariff object, so that an adjustment completely removed the effects of any previously applied adjustments.

The customer system may apply a tariff by repeatedly invoking the `getCharge()` operation supported by that tariff every second, and adding the returned value to the cumulative charge. The parameters supplied to `getCharge()` depend on the kind of tariff currently in force. For example, if the tariff is an implementation of `PacketCountTariff`, then measurements of inbound packets, outbound packets and congestion over the past second are required. However, if the tariff is an implementation of `RsvpTariff`, then only a `TSPEC` describing the current reservation is required. This implies that a customer system can only subscribe to a product if it can supply the parameters require by the tariff associated with hat product.

Each invocation of the `getCharge ()` method also results in an update to the tariff-specific user interface. For example, in the `CongestionSensitiveLinear` tariff, the usage parameters supplied to `getCharge ()` are used to update the graphical displays of traffic and congestion.

The announcement protocol is used to communicate serialised tariffs and adjustments from a provider system to multiple customer systems. The number of customer systems is assumed to be large, and a repeated multicast solution is adopted.

Each product supported by a provider is assigned a multicast channel for announcement purposes. Customer systems listen to the channels corresponding to the products that they are using. In the current implementation, it is assumed that each customer system has knowledge of well-known multicast addresses for the products it is interested in.

For each product channel, the provider repeatedly announces the current tariff and the most recent adjustment made to it (if any). Each announcement carries a version number, which is incremented each time the announcement is changed. Customer systems only process announcements when a version number change is detected. If a new customer joins a channel, it waits until it receives a tariff before processing any adjustment announcements. Furthermore, an adjustment is only applied if its announcement version is greater than that of the current tariff, thereby ensuring that a missed tariff announcement does not result in the application of a subsequent adjustment to an old tariff.

While centralised monitoring and control of tariffs by the network management platform is effective to respond to global changes in the loading of the network, it is difficult to handle localised congestion in this way. It is difficult to cause a price rise signal to be multicast in such a way that the signal is only received by those attempting to communicate packets through the point of congestion. This would require a separate multicast transmission for each element in the Internet , e.g. a multicast for every different queue on every interface of every router. Alternatively some aggregation of price rises triggered by local resource loading might be used. This however would mean that price rise signals were sent to users who were not making use of the congested resource. This in turn would make it necessary for the

price rise signal to be damped, reducing the ability of the price rise to reduce the demand on the congested resource.

To overcome these difficulties, the tariff algorithms installed on the customer terminals are arranged to respond automatically to congestion in a network resource being used by the terminal. Each algorithm includes a function which varies the price for network usage in dependence upon the detected congestion level. This function may be integrated in the main tariff algorithm, or, as in the example described here may be a separate algorithm used to calculate a premium to be added to a price calculated in accordance with the main tariff algorithm.

The main tariff algorithm calculates a price P as a function of a number of quality parameters, $Q_1$, $Q_2$, $Q_3$ where, for example, $Q_1$ is a specified latency for packets communicated across the interface between the customer terminal and the network, $Q_2$ is the reserved bandwidth for the transmission, $Q_3$ is a specified level of reliability corresponding to a maximum permissible level of packet loss.

The price P is then given by:

$$P = f(Q_1, Q_2, Q_3, \ldots\ldots)$$

An example of the pricing function in terms of one of the quality parameters Q is shown schematically in Figure 2a.

The congestion tariff algorithm calculates a premium $\Delta P$ which is a function of one or more congestion parameters C:

$$\Delta P = f(C_1, C_2 \ldots)$$

The congestion parameters provide a measure of the loading of the resources which a customer terminal is making use of at any given time. In the present example the ratio of packets lost to packets received is used as the congestion parameter. This parameter is readily calculated, for example in the case of packets using TCP (transport control protocol), or RTP (real time protocol) over UDP (user datagram protocol), since such packets include a sequence number. Figure 2b shows one example of the function for generating the premium. In this case, the premium increases as an approximately exponential function of the congestion, so that at low congestion levels a small premium is charged, while if congestion increases still further, then at higher levels of congestion the premium increases sharply.

In an alternative implementation, an explicit congestion signal is added by any congested router within the network to packets transmitted to the customer

terminal. Whether congestion is signalled explicitly or implicitly by packet drop, the price algorithm might not directly charge for congestion indication. Instead, it may charge if the customer terminal does not halve the congestion window in response to a congestion indication. Halving the congestion window halves the rate of transmission which is the standard response to congestion indication used in TCP and other compatible congestion control protocols. The change in transmission rate can be measured by the network provider as well as at the customer terminal, although this places a heavy load on router processing resources. If the provider is merely sampling certain customers to audit their own measurements, this results in an acceptable load.

Although only a single main tariff and premium are described here, in practice different subdomains, and different service providers associated with each subdomain, may each have a different pricing structure, with different main and premium tariffs. However, there is across all the subdomains a common relationship between network loading levels and congestion signalling.

The operation of this second implementation will now be described in the context of a network operating using a differentiated service as described in the Internet Engineering Task Force draft "Differentiated Services Operational Model and Definitions" and in the paper by David D Clark (MIT), "A Model for Cost Allocation and Pricing in the Internet", presented at MIT Workshop on Internet Economics, Mar 1995, URL:http://www.press.umich.edu/jep/works/ClarkModel.html. In a network implementing differentiated services, nodes are arranged to discriminate between packets to provide different levels of service. This capability might be used, for example, to accord delay-sensitive data, such as data generated by an IP telephony client, a higher priority compared to other data, such as email data. At the network edge, for example at a client terminal running the IP telephony client, bits in a TOS (type of service) octet contained within each packet header are set to indicate the appropriate service level. Those bits are used by routers within the network to determine how the relevant packets should be handled.

The TOS octet when used in this way is termed the DS (differential service) byte. The format of the differential service byte is shown in Figure 3. Bit zero, labelled "IN" indicates whether the packet is inside or outside a defined profile. Bits 1 to 5 labelled "PHB" define a "per-hop-behaviour" that is they indicate how, for

example, a router should handle the packet, e.g. by according it lower or higher priority. Bits 6 to 7, in this particular form of the DS byte, are used for explicit congestion notification (ECN). One of these bits is set to indicate whether the routers in the path of the packet are capable of setting the ECN field, and the other bit is used as a flag which is set (by ECN capable routers) when congestion, or loading which would potentially lead to congestion, occurs. Random Early Detection (RED) algorithms are currently implemented in routers. These algorithms measure average queue length within the packet buffers of a router. An exponential moving average is calculated. When that average queue length exceeds a predetermined threshold, then the router signals that congestion is occurring. Conventionally this signalling has been done simply by dropping a packet. However, in the context of an ECN scheme, the router, instead of dropping a packet, sets an ECN bit in a packet header to indicate that congestion is occurring. This is done probabilistically: that is, some only of the packets passing through the router are marked. The probability of a packet being marked increases with the average queue size. In the rare case that the queue increases to a length where the router buffers are full, then packets are dropped, rather than an ECN bit being set. In this case ECN bits are set for all the remaining packets.

In operation, if the client terminal 5 is accessing a data source on the server 9, congestion may occur, for example, at router 4 which links network sub-domains 2B and 2C. RED-like algorithms in the router 4 detect that the queue lengths in the router buffers, as calculated using the exponential moving average, exceed a predetermined threshold. Accordingly some of the packets from the server 9 en route to the client terminal have the ECN bit of the DS byte set by the router 9 to mark the fact that congestion is occurring. At the client terminal, the DS byte in the headers of incoming packets is read. A moving average of the number of packets containing an ECN bit which is marked is calculated. This average then provides the congestion parameter $C_i$, which is used to calculate the premium:

$$\Delta P = f(C_i).$$

The total price to the user $P_{TOT}$ is then calculated by adding together the prices determined by main tariff algorithm and by the premium algorithm:

$$P_{TOT} = P + \Delta P.$$

This total price is passed to a cost decision agent running on the client terminal. This cost decision agent is programmed with user defined rules. These might state, for example, that the cost decision agent should authorise the system to proceed with a connection as long as the total cost averaged over a certain time period falls below a predetermined threshold, e.g. of £0.01 per minute, and that the cost decision agent should suspend a connection and alert the user if the cost rises above that threshold. Alternatively, as previously noted, the cost decision agent may handle several applications simultaneously, and may be programmed to slow down one of the applications as the premium for using a data source accessed by that application increases.

For some customers in some circumstances, the variability of the tariff for network usage may pose problems. For example, a customer might wish to schedule a multicast audio-video conference with, say, twenty participants and with the customer intending to pay the network usage costs for all of the participants. The conference will be scheduled a day or more in advance, but since the tariff is variable over time, at the point when the conference is scheduled, the customer will not know the cost which will be incurred. The preferred implementation of the present invention overcomes this problem for the customer, and also provides an additional revenue source for the network operator. This is achieved by applying a further tariff which defines a premium for price stability for a given customer terminal, the value of the premium increasing as the required duration of the period of stability increases. In the example referred to above, the customer scheduling a conference one day in advance refers to the current tariff to determine the present cost of the network resources required, including any congestion premium currently applicable, and then refers to the further tariff to determine the premium for maintaining the cost at its present value for a period of one day. Then if the user decides to make use of the fixed tariff a message is sent from the user to the network operator. The message identifies the data flows in question, for example by specifying the IP addresses and the service levels for the audio and video data flows between the participants, together with the current time at which the user is contracting for a fixed period, and the required duration of the fixed period and also an identifying code for the message. Alternatively, the message with these details may be tracked with an appropriate cryptographic function (e.g. MD5), and the hash value only communicated initially to

the provider, and subsequently used to verify account data. Subsequently, for the duration of the specified period, in this case one day, the user applies the fixed tariff. In systems where the users themselves are responsible for generating accounting data and calculating the applicable charge for network usage, then the user calculates the charge using the fixed tariff and returns the accounting data to the network operator together with the identifying code for the fixed tariff contract.

This aspect of the invention is not only applicable to systems where tariff variation is carried out locally in response to the detection of congestion, but may also be used in systems where, for example, the only variation is imposed by the network operator.

The tariff for the stability premium may be distributed by multicasting from tariff entities in network operator platforms to the customer terminals in the same manner as described previously for the other tariffs discussed above. As with those other tariffs, different tariffs and optionally different periods of stability might apply to different service levels. In a scenario such as that discussed in the preceding paragraph, then different service levels might be used for different elements of the audio and video data streams required for the multicast conference.

Figure 2c shows a possible for the stability premium tariff. This tariff may be embodied in a Java function multicast to the users. Curve C is communicated to the customer terminal as another subsidiary algorithm that contributes to the main tariff algorithm. The customer may choose a period of price stability and calculate the premium above the spot price that his will require using curve C. Curve B is an example of the stable price chosen in a particular case. Once the period of stability expires a new one can be bought at the premium over the spot price at that time. To buy a period of price stability, the customer must announce the period required and the range of addresses for which it applies to her provider. It may be required for one address (e.g. for the duration of an Internet phone call to a single person) or for a range of addresses (e.g. for a video conference). Certain risk-averse customers might request stable pricing for all addresses all the time.

For ease of description, the preceding sections have treated in isolation the local variations in tariff in response to congestion. In practice, this mechanism will in general be combined with other responses to congestion, and with other sources of variation in the tariff. Also, a decision to proceed with a transmission despite

congestion will in general require the consent of parties at both ends of the transmission. Considering the entire system of the data source, network and routers and the data receiver, the implementation of an increase in tariff (also termed here a "fine") in response to locally detected congestion occurs as a last resort. Other responses are implemented first, in the following numerical order:

1.the network re-routes around congestion

2.the network borrows capacity from lower levels of service (lower in the context of the relevant dimension(s) of QoS) including the best effort service

3.the network introduces extra capacity (possibly automatically)

4.the end-system establishes that the congestion is on the shared network and not just on the access links or end systems

5.the end-system sets QoS requirements to a "higher" level (if cheaper than the fine for ignoring congestion at the current level)

6.the end-system decides it is essential to ignore the congestion, given the fine for doing

so might be quite high

7.both (all) end-systems agree to ignore the congestion.

Typically, it is at step 4 that an ECN signal is generated. Steps 1 to 3 precede the generation of this signal and steps 5 to 7 follow the generation of the ECN signal.

The last step prior to proceeding with a connection and paying the premium for doing so is establishing agreement by both parties. Accordingly, when the customer terminal detects congestion, either through receiving explicit congestion notification, or through detection of a relevant parameter such as packet loss, the customer terminal signals this fact back to the or each other end system. In the present example therefore, the client terminal 5 signals to the data server 9 that congestion is occurring. The data server is programmed with rules, which as at the customer may be implemented as an agent, which determine the response to such a signal. For example, the server may refuse service in these conditions. As described previously with respect to Figure 1, in the present example tariffs are multicast through the network from network operators to the customer terminals, and charging is carried out using a "pay and display" process. Figures 4a and 4b shows the objects used to implement the charging architecture in this case. Figure 4a

shows the higher level objects and 4b shows the component objects used in a software implementation of the architecture of Figure 4b. In Figure 4a, objects on the client terminal are shown in the half of the Figure labelled "customer" and objects on the access router 7 and the corresponding network sub-domain are shown in the half of the Figure labelled "edge network". The objects on the customer terminal include a session control object S, a customer business rules object $B_c$, a customer pricing object $Pr_c$, a QoS manager Q, a customer accounting object $Act_c$ and a customer measurement object $M_c$. The business rules object $B_c$ receives information on those aspects of the session which involve liability for payment and receives current pricing data from the pricing object $Pr_c$. The customer business object makes decisions, under the customer's policy control on which chargeable services are utilised, and how much of the chargeable services are utilised. These decisions are fed to the QoS manager Q, which decides which mechanisms are used to achieve the requirements. The QoS manager then controls the customer measurement object $M_c$ to determine which aspects of traffic and service to measure and which aspects to ignore. The measurement object then records the selected aspects of the traffic, for example counting the number of packets received by the customer terminal and the QoS levels for those packets. These data together with the current tariffs, including any premium for congestion, are then used by the customer terminal to determine the charge payable to the network operator. The measurement object $M_c$ is also programmed with instructions which determine the frequency with which it passes data to the customer accounting object $Act_c$. The customer accounting object $Act_c$ passes payments to an accounting object $Act_p$ in the network provider's domain.

The accounting objects on the customer terminal may be implemented using a small encrypted flat-file database. On the network provider's side, the equivalent objects may be implemented using a larger database that is scaleable to handle e.g., tens of thousands of customer accounts. An object request broker (ORB) is used for communication between the customer-side objects and the network-side objects, implemented using commercially available tools such as ORBIX (TradeMark) from Iona Technologies plc.

On the network provider's side, that is to say within the subdomain to which the customer terminal is connected, the customer's traffic is measured by a version of $M_c$ denoted $M_p$, but only on a sampling basis determined by the policing function,

Po. That is to say, the network operator samples the customer's traffic only intermittently. Po controls where in the network measurements are made in order to capture all of any particular customer's traffic. A bulk measurement function, $M_b$, is responsible for reporting aggregate traffic levels, as reflected in the moving average of the router queue lengths, to the pricing object, $Pr_p$. Bulk measurements would typically be collected from across the provider's domain to a centralised pricing function (which would be replicated for reliability). $Pr_p$ sets prices taking into account the business rules from the network provider's business object, $B_p$, as well as the current traffic levels reported by Mb and pricing from neighbouring providers (see below). The policing function, Po, compares sample measurements from $M_p$ with accounting messages received at $Act_p$ as a result of the customers own measurements . If it establishes that the accounts are insufficient it might restrict service at the access control gateway, Acs, or initiate some other punishment. Encapsulated within the accounting object another policing object checks the accounts match the payments within the contracted time for payment. Finally, the identity mapping function, I, provides a mapping between a customer's identity (account, digital signature, etc.) and their current network address (typically allocated by the ISP, whether unicast or multicast).

Figure 5 shows the data which are passed between the accounting objects. In this example the account data comprises: account identity; bill record identity; service type identifier; source address; destination address; tariff identity; time; period (i.e. the period covered by the bill record); units; cost; and currency. In addition, the payment data comprises the amount of money and the currency of payment.

Figure 6 shows the measurement region within protocol stacks on the customer terminal and in the network domain. Ideally there would be two measurement points within this region, one trusted by the customer and one trusted by the network, for example at the two points referenced (a) in the Figure. For ease of implementation, a single measurement point (b) trusted by both parties may be used. This might be implemented, for example within a secure module such as a cryptographic card on the client terminal. As an alternative, measurements may be made at different points with some possibility of discrepancies between measurements. On the network the practical measurement point is at the first

access device(s) that, for each customer, inspects network layer headers (c)(IP in this case). ISPs should not measure any deeper into their network (d) because their access network and systems will introduce delays and losses.

For an individual customer (e.g. on dial-up access), a practical point at which to measure would also be alongside the network layer but in their end-system's stack (e). Ideally these measurement points would be lower in each stack to be closer to the interface between the two parties and less likely to be affected by contention in the stack. However, measuring at the link layer (f-f) would be inappropriate because only some chargeable parameters set at the network layer will ever be reflected in link layer frames; network level multicast, end-end latency requirements etc. may never be visible at the link layer. Also, link layer headers would need to be ignored when measuring packet sizes for bandwidth calculations to avoid apparent discrepancies where different link technologies are chained together.

In the reception direction (up the stack) this choice of measurement points implies that the lower layers must be dimensioned (buffer sizes, interrupt and thread scheduling priorities) to cope with the most stringent QoS requirements of higher layers. As frames are taken off the physical media, the machine must be able to pass data up the stack without any chance that usage-charged data gets discarded (e.g. due to buffer overflow caused by interrupt contention) before it gets to the network layer. It is at the network layer where the ISP's service is to be measured and where it is most convenient for QoS requirements to control correct differential treatment of the various flows as they are passed further up the stack (on end-systems) or forwarded (on routers).

The measurement objects described above may be implemented using, with appropriate modifications, publicly available network metering software such as Nevil Brownlee's NeTraMet system. This is a software meter which conforms to the IETF internet accounting architecture described in RFC 2063 and RFC 2064. The meter builds up, using "packet sniffing", packet and byte counts for traffic flows, which are defined by their end-point addresses. Although generally, Addresses can be ethernet addresses, protocol addresses (IP, DECnet, EtherTalk, IPX or CLNS) or 'transport' addresses (IP port numbers, etc), or any combination of these, in the present implementation IP addresses only are used. The traffic flows to be observed are specified by a set of rules, which are downloaded to NeTraMet by a 'manager'

program. Traffic flow data is collected via SNMP (Simple Network Management Protocol) from a 'collector' program.

Figure 7 shows how the main tariff determined by the network operator varies in time. In the Figure, curve A is the spot price calculated to reflect the loading of the network at any instant. Curve B is one of a number of different tariff bands. Different tariff bands have different volatilities, and the customer pays a premium for bands offering greater stability. Tariffs are communicated to the customer terminals using a hierarchy of channels carried by the network. An initial contract between a customer and a service provider a single channel address that might typically hold new announcements distributed some months apart (e.g. for contract variations or for new services specifying which second level channel to listen to for tariffs or for downloading new code to handle new tariff structures). The second level channels might deliver updates hours apart which simply announce the addresses of third level channels for the most volatile information. These third level channels may carry updates at intervals of less than a second. Prices for many services may be carried on one channel. For greatest efficiency, this one channel may be split into several channels at times of highest volatility, and re-aggregated into a single channel in more stable periods.

Tables 1 to 7 below list Java source code used to implement two different tariffs. The code of table 1 establishes the operations used for communication between a customer system and a tariff algorithm downloaded by the customer system. Table 2 shows a linear tariff algorithm, in which the tariff depends on the total of the packets sent and packets received by the customer together with a congestion parameter. Table 3 shows the code for generating the customer display in this case. Table 4 shows the code used to display the tariff at the network operator's server. Table 5 shows an exponential tariff algorithm. Table 6 generates the customer display and Table 7 the operator display for the exponential tariff algorithm. By downloading Java code to generate the user interface, that interface can be tailored to the requirements of the particular tariff, and can be adapted as the tariff changes.

Although the examples so far described have been in the context of federated packet data networks, such as the Internet, many aspects of the invention can also be used with advantage in other types of network, such as in a circuit-

switched PSTN (public switched telephony network). Figure 11 shows an example of the invention applied in this context. In this network, customer terminals 81, which are in this example so-called intelligent phones, that is telephones incorporating a microprocessor and a data interface, are connected via local exchanges 82 and trunk exchanges 3 to the telephony networks. The trunk exchanges 83 are connected via a common channel SS7 (signalling system number 7) signalling network to a service control point 85 that is responsible for the execution of advanced call control functions. The service control point 85 is also connected to an operational support server 86 that is responsible for billing operations, and that, in this example, controls the setting of tariffs for the network. The OSS server and customer terminals include tariff entities (TE). The fixed PSTN network is also interconnected via a gateway 87 to a cellular GSM network 88. Base Stations BS in the cellular network communicate signals to intelligent mobile phones 89. In operation, network tariffs are distributed to customer terminals via the PSTN network and via the GSM network. Conveniently, the tariff may again take the form of Java functions which are executed on processors in the customer terminals. The Java functions may be streamed as Internet packets. In one implementation, these Internet packets may be distributed via the PSTN networks and GSM networks themselves. For example, the packets may be encapsulated and transported to the trunk exchanges using the MTP (message transport part) transport layer and may be communicated onwards to the customer terminals using out-of-band signalling. Alternatively, a separate data connection may be established between the OSS server and the customer terminals via the public internet. As in the examples above, the network operator monitors the loading of resources within the network and may transmit signals to the tariff entities in the customer terminals to change the tariff to reflect the scarceness or otherwise of relevant resources. Customer terminals may themselves monitor network loading and automatically generate variations in the tariffs. Usage of network resources may be measured locally by the customer terminals instead of conventional billing carried out within the network. The network operator may police the measurement of usage data by carrying out sampling, as described previously.

Table 1

```
// Generated by Together
package com.bt.jungle.lsma.charging.pricing;

import com.sun.java.swing.JComponent;

/**This establishes the operations used for
communication between the customer system
and the downloaded algorithm.
@author Mike Rizzo*/
public interface Tariff {
Jcomponenet getGUI( );
Float getPrice (int pkin, int pkout, int cng);
```

Table 2

```
package algorithms.linear;

import com.sun.java.swing.JComponent;
import com.sun.java.swing.JTextField;

import com.bt.jungle.isma.charging.pricing.Tariff ;

public class LinearAlgorithm implements Tariff {
        private float rate;
        private LinearAlgorithmDisplay display;
        public LinearAlgorithm ( ) {
                display = new LinearAlgorithmDisplay ( );
                setRate (new Float(1));
        }
        public float getPrice (int pkin, int pkout, int cng) {
                return (pkin + pkout + cng) * rate;
        }
        public JComponent getGUI( ) { return display; }
        public void setRate (Float f) {
                rate = f.floatValue( ) ;
                display.setRate (rate) ;
        }
}
```

Table 3

```
// Generated by Together

package algorithms.linear;

import com.sun.java.swing.JPanel;
import com.sun.java.swing.JTextField;
import com.sun.java.swing.Box;
import com.sun.java.swing.JLabel;

public class LinearAlgorithmDisplay extends Jpanel {
        private JTextField tfRate = new JTextField (4);
        public LinearAlgorithmDisplay ( ) {

                Box vbox = Box.createVerticalBox ( ) ;

                Box hbox = Box.createHorizontalBox ( ) ;
                hbox.add (Box.createHorizontalGlue ( )) ;
                hbox.add (new Jlabel ("Rate:"));
                hbox.add (Box.createHorizontalGlue( ));
                hbox.add (tfRate);
                tfRate.setEditable (false);
                hbox.add (Box.createHorizontalGlue( ))
                vbox.add (hbox);

                add (vbox());
        }
        public void setRate (float f) {
                tfRate.setText (String.valueOf (f));
        }
        }
```

Table 4

```
// Generated by Together
package algorithms.linear;

import com.sun.java.swing.*;
import java.awt.event.*;

import com.bt.jungle.isma.charging.pricing.provider.*;
import com.bt.jungle.util.*;

public class LinearAlgorithmGUI extends Jpanel {
        private JTextField tfRate - new JTextField ( );
        private TuningMessageListener tuningMessageListener;
        private final static String DEFAULT_RATE = "1.0";
        public LinearAlgorithmGUI (TuningMessageListener tml) {
                tuningMessageListener = tml;
                tfRate.setText (DEFAULT_RATE);

        Box vbox = Box.createVerticalBox( );

        Box hbox = Box.createHorizontalBox ( );
        hbox.add (new Jlabel ("Rate:"));
        hbox.add (Box.createHorizontalGlue( ));
        hbox.add (tfRate);
        hbox.add (Box.createHorizontalGlue( ));
        hbox.add (hbox);

        JButton bTransmit = new JButton ("Transmit");
        bTransmit.addActionListener (
                new ActionListener ( ) {
                        public void actionPerformed (ActionEvent e) {
                                transmit ( ) ;
                        }
                }
        );
        hbox = Box.createHorizontalBox( );
        hbox.add. (Box.createHorizontalGlue( ));
        hbox.add (bTransmit);
        hbox.add (Box.createHorizontalGlue( ));
        vbox.add (hbox);

        add (vbox);
}
void transmit ( ) {
        try {
                Float f = new Float (tfRate.getText( ));
                Object  args [ ] = new Object [1];
                Args [0] = f;
                TuningMessageListener.notify(
```

```
                        new Invocation ("SetRate", args)
                    };
                }
                catch (Exception e) {
                    e.printStackTrace ( );
                }
            }
        }
```

Table 5

```
package algorithms.exp;

import com.sun.java.swing.JComponent;
import com.sun.java.swing.JTextField;

import com.sun.java.lsma.charging.pricing.Tariff;

public class ExpAlgorithm implements tariff {
        private float min;
        private float base;
        private float divisor;
        private ExpAlgorithmDisplay display( );
        public ExpAlgorithm( ) {
                display = new ExpAlgorithmDisplay ( );
                setMin (new Float (1));
                setBase (new Float (2));
                setDivisor (new Float (10));
        }
        public float getPrice (int pkin, int pkout, int cng) {
                return min + (float)math.pow (base,(pkin + pkout + cng)/divisor);
        }
        public JComponent getGUI( ) {return display; }
        public void setMin (Float f) {
                min = f.floatValue( );
                display.setMin(min);
        }
        public void setBase (Float f) {
                base = f.floatValue( );
                display.setBase(base);
        }
        public void set Divisor (Float f) {
                base = f.floatValue( );
                display.setBase (divisor);
        }
}
```

Table 6

```
// Generated by Together

package algorithms.exp;

import java.awt.GridLayout;
import com.sun.java.swing JPanel;
import com.sun.java.swing.JTextField;
import com.sun.java.swing.Box;
import com.sun.java.swing.JLabel;

public class ExpAlgorithmDisplay extends Jpanel {
        private JLabel tfDisplay = new JLabel ( );
        private float min, base, div;

        public ExpAlgorithmDisplay ( ) {

                add (tfDisplay);
        //              tfDisplay.setEditable (false);
                updateDisplay ( );
        }
        private void updateDisplay ( ) {
                tfDisplay.setText ("price = " + min + " + " + base +
"^((pkin+pkout+cng)/" + div +")");
        }
        public void setMin (float f) {
                min = f;
                updateDisplay ( );
        }
        public void setBase (float f) {
                base = f;
                updateDisplay ( );

        public void setDivisor (float f) {
                div = f;
                updateDisplay ( );
        }
}
```

Table 7

```
// Generated by Together

package algorithms.exp;

import java.awt.GridLayout;
import com.sun.java.swing.*;
import java.awt.event.*;

import com.bt.jungle.isma.charging.pricing.provider.*;
import com.bt.jungle.util.*;

public class ExpAlgorithmGUI extends Jpanel {
        private JTextField tfMin = new JTextField ( );
        private JTextField tfBase = new JtextFfield ( );
        private JTextField tfDivisor = new JTextField ( );

        private TuningMessageListener tuningMessageListener;
        private final static String DEFAULT_MIN = "1.0";
        private final static String DEFAULT_BASE = "2.0";
        private final static String DEFAULT_DIV = "10.0";

        public ExpAlgorithmGUI (TuningMessageListener tml) {
                tuningMessageListener = tml;
                tfMin.setText (DEFAULT_MIN);
                tfBase.setText (DEFAULT_BASE);
                tfDivisor.setText (DEFAULT_DIV);

                Box vbox = Box.createVerticalBox ( );

                vbox.add (new JLabel ("price = min + pow (base,
(pkin + pkout + cng)/divisor)"));

                vbox.add (Box.createVerticalGlue ( ));

                Jpanel panel = new JPanel (new GridLayout (3,2));
                panel.add (new JLabel ("Minimum"));
                panel.add (tfMin);
                tfMin.addActionListener (
                        new ActionListener ( ) {
                                public void actionPerformed (ActionEvent e) {
                                        transmit ("setMin", tfMin);
                                }
                        }
                );
                panel.add (new JLabel ("Base"));
                panel.add (tfBase)
                tfBase.addActionListener (
                        new ActionListener ( ) {
```

```
                        public void actionPerformed (ActionEvent e) {
                        transmit ("setBase", tfBase);
                    }
                }
            };
            panel.add (new JLabel ("Divisor"));
            panel.add (tfDivisor);
            tfDivisor.addActionListener (
                new ActionListner ( ) {
                    public void actionPerformed (ActionEvent e) {
                        transmit ("setDivisor", tfDivisor);
                    }
                }
            );
            vbox.add (panel);

            add (vbox)
        }
        void transmit (String m, JTextField tf) {
            try {
                Float f = new Float (tf.getText ( ));
                Object args [ ] = new Object [1];
                args [0] = f;
                tuningMessageListener.notify(
                    new Invocation (m, args)
                );
            }
            catch (Exception e) {
            e.printStackTrace ( );
            }
        }
    }
```

CLAIMS

1. A method of operating a communications network, including automatically varying, depending on network loading as detected at a customer terminal, a tariff for network usage by the customer terminal.

2. A method according to claim 1, including detecting at the customer terminal a network performance parameter which depends on network loading, and varying the tariff depending on the network performance parameter.

3 A method according to claim 2, in which the network is a packet network and the network performance parameter is the number of packets lost in transmission between a data source and the customer terminal.

4. A method according to claim 1, including detecting a congestion signal at the customer terminal and varying the tariff in response to the congestion signal.

5. A method according to claim 4, including reading a congestion signal at the customer terminal from a data packet received at the customer terminal.

6. A method according to claim 4 or 5, including generating a congestion signal at a router in the network in response to the detection of congestion at the router.

7. A method according to any one of the preceding claims, including making a first relatively smaller increase in the tariff when congestion is first detected, and making at least one further, relatively larger increase, if the congestion persists.

8. A method according to any one of the preceding claims, including programming a decision agent at the customer terminal with user-determined price criteria, and comparing a price calculated using the tariff with the said price criteria.

9. A method according to any one of the preceding claims, including distributing a tariff algorithm via the communications network to a plurality of terminals and

calculating at each terminal, using the tariff, a charge for network usage by the terminal.

10. A method according to claim 9, further comprising steps, carried out by the network operator, of:

intermittently sampling traffic between a customer terminal and the network, and as part of the sampling recording network loading affecting the customer terminal; and

for the sampled traffic comparing a charge calculated by the customer terminal and an expected charge and detecting thereby any discrepancy.

11. A method according to any one of the preceding claims, in which when the customer terminal detects congestion in data transmitted to the customer terminal from a data source via the network, the customer terminal returns a congestion notification signal to the data source.

12. A method according to any one of the preceding claims, including at a customer terminal, selecting a period of time for which the tariff is to be fixed and paying a premium depending on the duration of the said period.

13. A method of operating a communications network including applying to customer terminals a tariff for network usage, varying the tariff with time; at a customer terminal, selecting a period of time for which the tariff is to be fixed; and paying a premium depending on the duration of the said period.

14. A communications network including :

means for detecting network loading locally at a customer terminal; and

means responsive to the said means for detecting arranged automatically to vary a tariff for network usage by the customer terminal.

15. A customer terminal for use in a communications network, the customer terminal including:

means for detecting loading of a network to which, in use, the customer terminal is connected;

means responsive to the said means for detecting and arranged automatically to vary a tariff for network usage by the customer terminal.

14. A customer terminal for use in a communications network, the customer terminal including one or more processors arranged to carry out the following steps in sequence:

detecting loading of resources in a network to which the customer terminal is connected; and

automatically varying in dependence on the detected loading a tariff for network usage by the customer terminal.

15. A method according to any one of claims 1 to 13, in which the tariff is varied only if the terminal fails to reduce its output in response to detected congestion.

Fig.1.

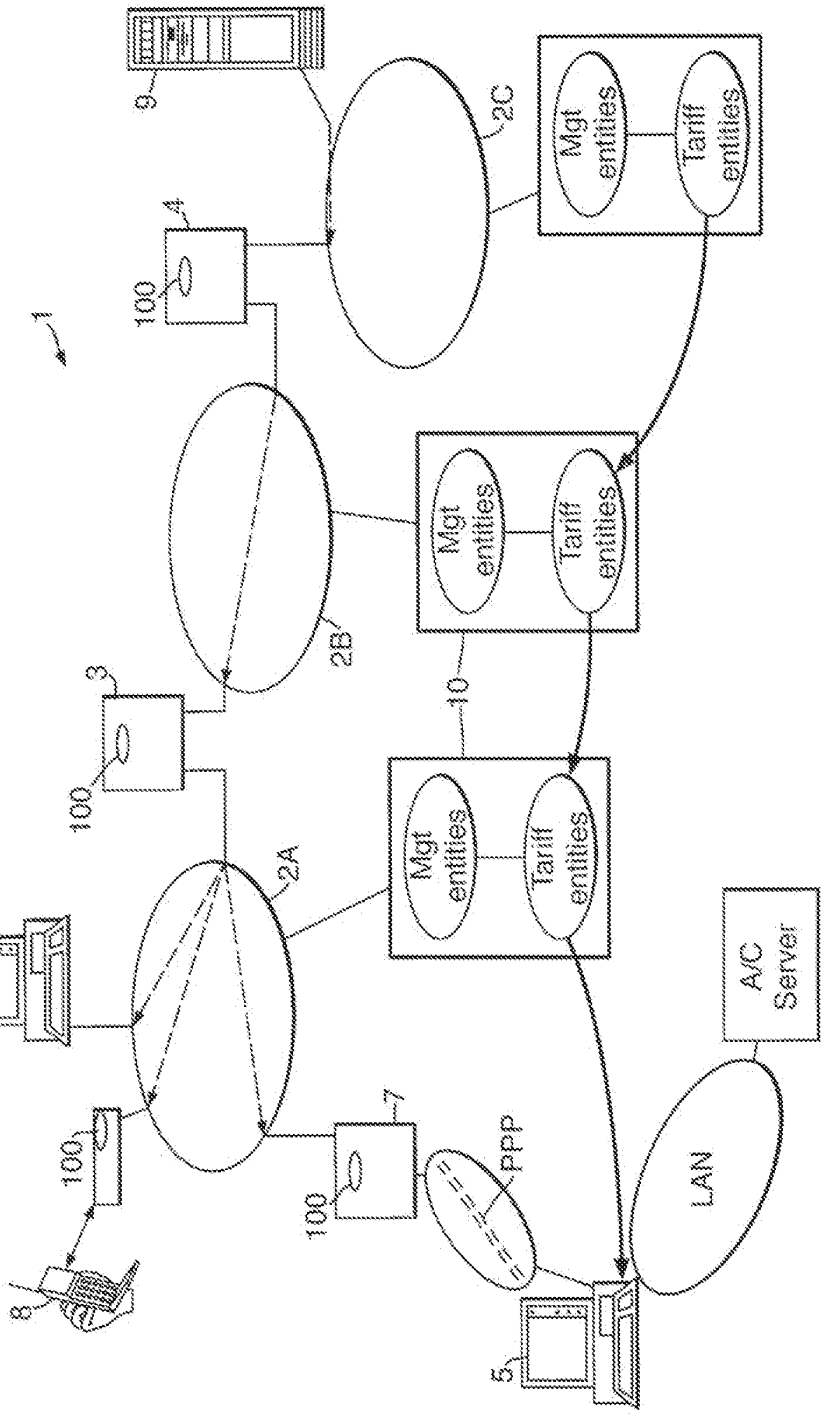

1
2A
2B
2C
3
4
5
7
8
9
10
100
Mgt entities
Tariff entities
A/C Server
LAN
PPP

Fig.2a.

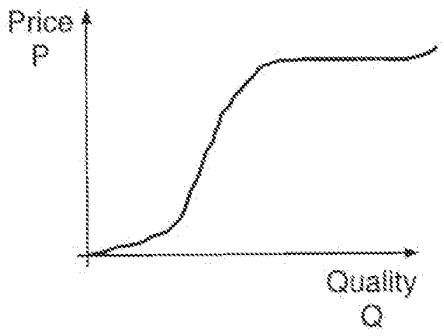



Fig.2b.

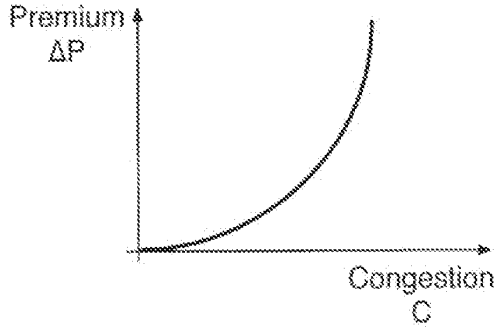



Fig.3.

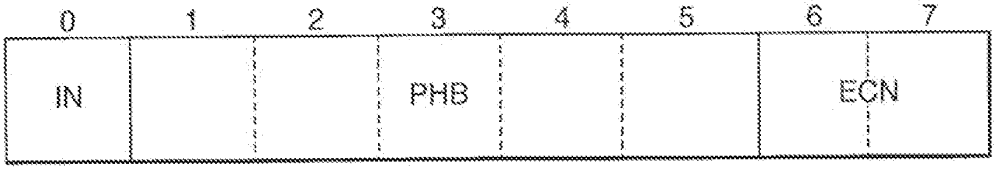


Fig.2c.

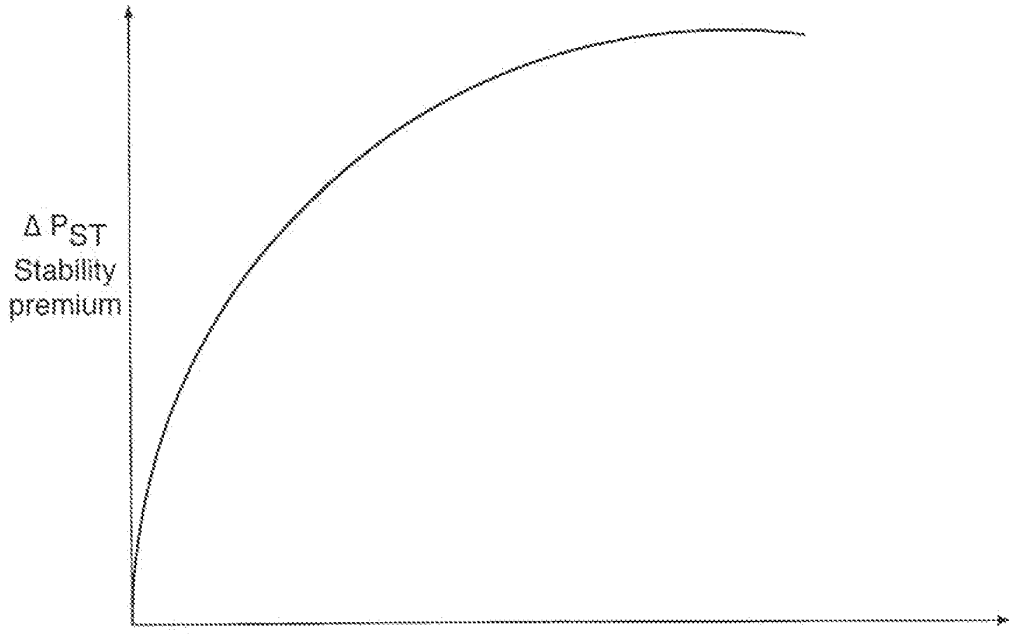


Fig.4a.

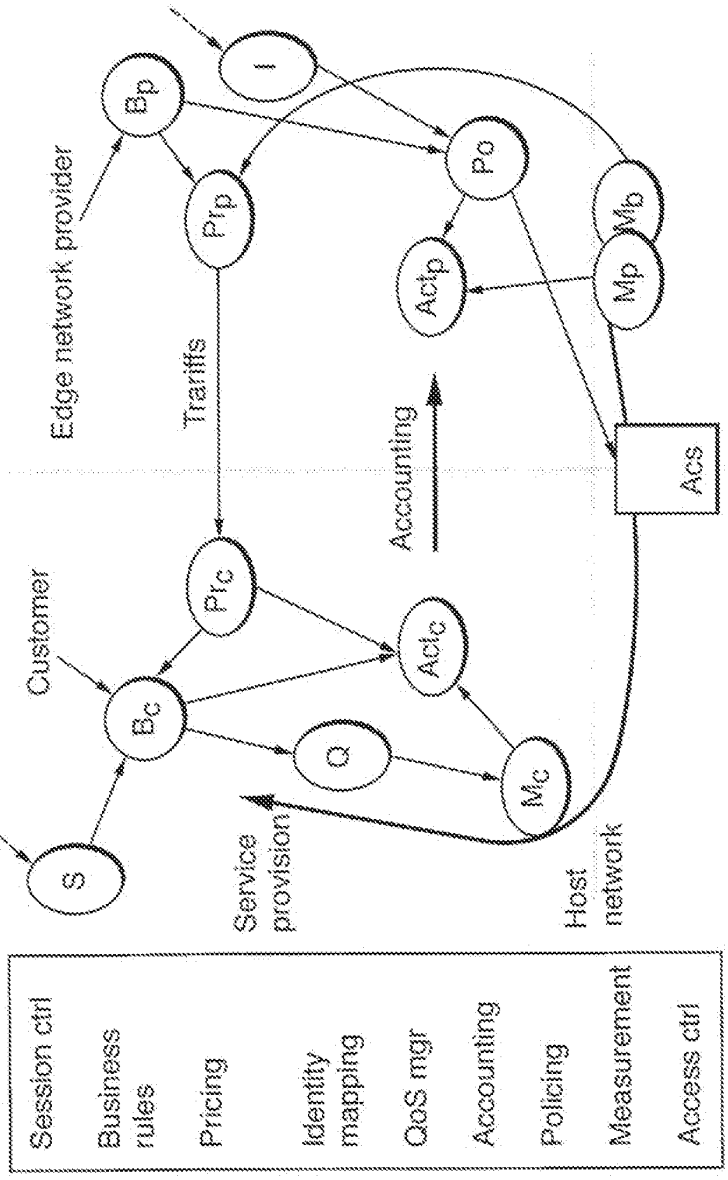

Session ctrl
Business rules
Pricing
Identity mapping
QoS mgr
Accounting
Policing
Measurement
Access ctrl
Customer
Edge network provider
Service provision
Host network
Tariffs
Accounting
S
$B_C$
Q
$M_C$
$Pr_C$
$Act_C$
$B_P$
$Pr_P$
I
$P_O$
$Act_P$
$M_P$
$M_O$
Acs

Fig.4b.

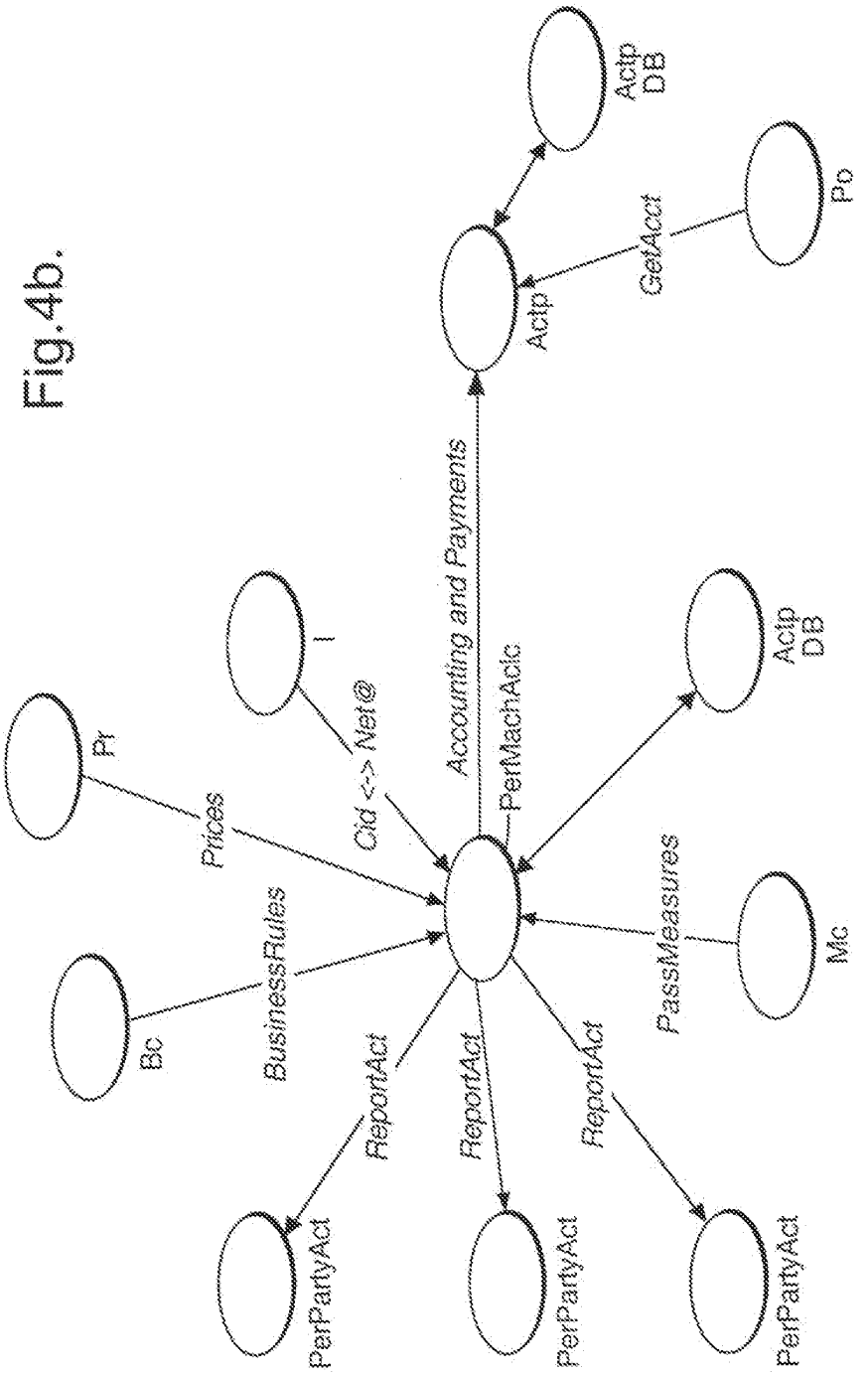

Actp DB
Po
GetAcct
Actp
Accounting and Payments
I
Pr
Prices
Oid <-> Net@
PerMachAcic
Actp DB
Bc
BusinessRules
PassMeasures
Mc
ReportAct
ReportAct
ReportAct
PerPartyAct
PerPartyAct
PerPartyAct

Fig.5a.

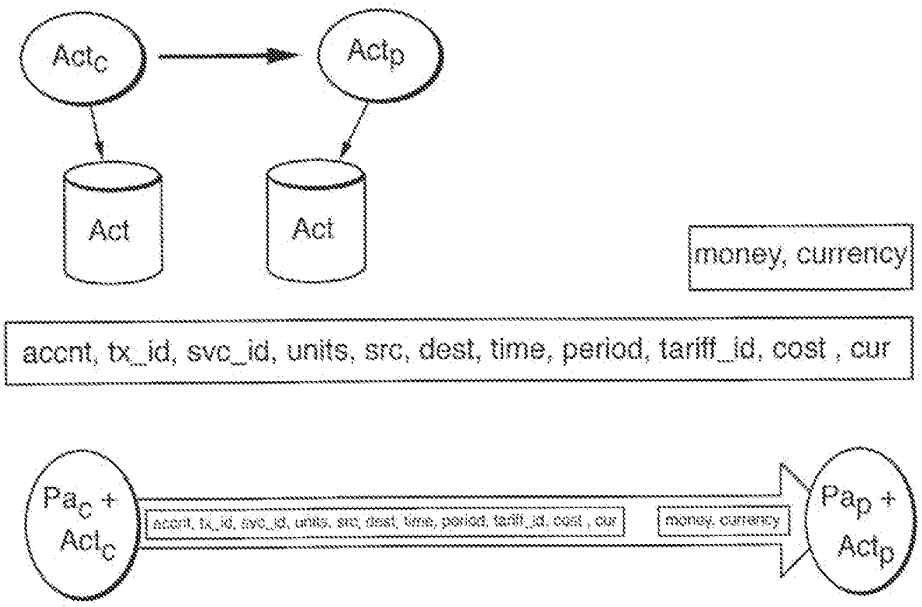

Act$_C$
Act$_P$
Act
Act
money, currency
accnt, tx_id, svc_id, units, src, dest, time, period, tariff_id, cost , cur
Pa$_C$ + Act$_C$
accnt, tx_id, svc_id, units, src, dest, time, period, tariff_id, cost , cur
money, currency
Pa$_P$ + Act$_P$

Fig.5b.

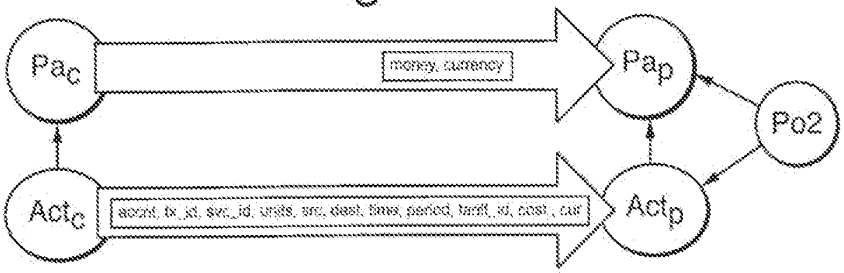

Pa$_C$
money, currency
Pa$_P$
Po2
Act$_C$
accnt, tx_id, svc_id, units, src, dest, time, period, tariff_id, cost , cur
Act$_P$

Fig.6.

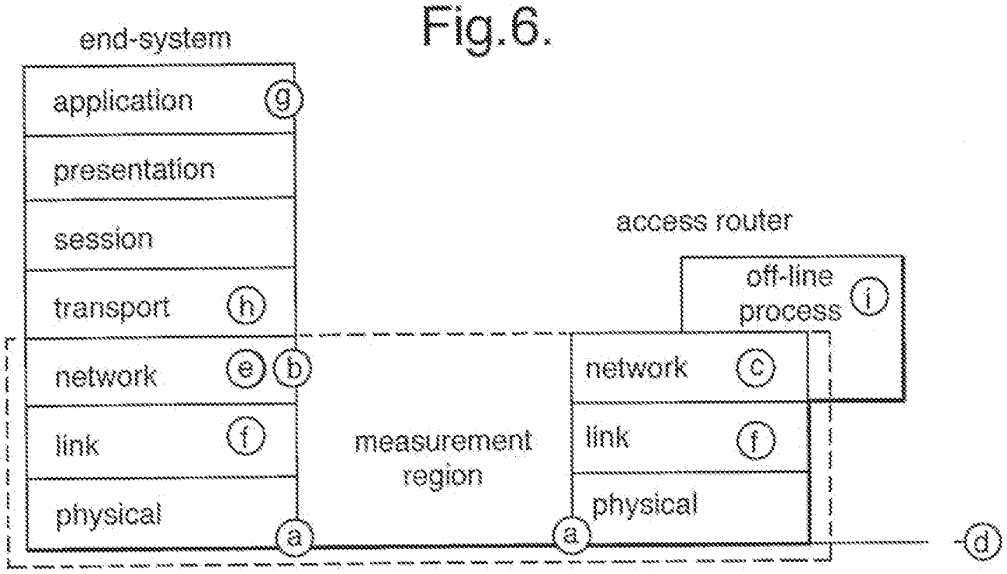

end-system
application
g
presentation
session
transport
h
network
e
b
link
f
physical
a
measurement region
access router
off-line process
i
network
c
link
f
physical
a
d

Fig.7.

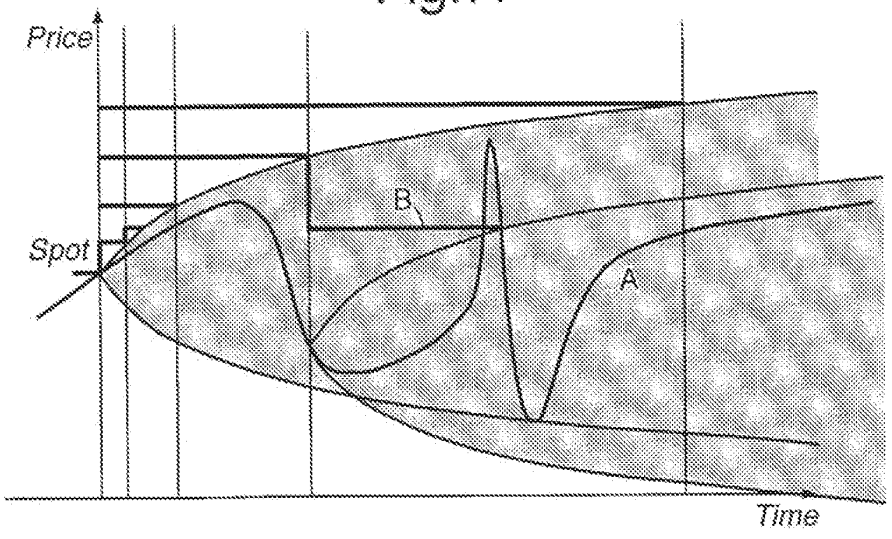

Price
Spot
B
A
Time

Fig.8a.

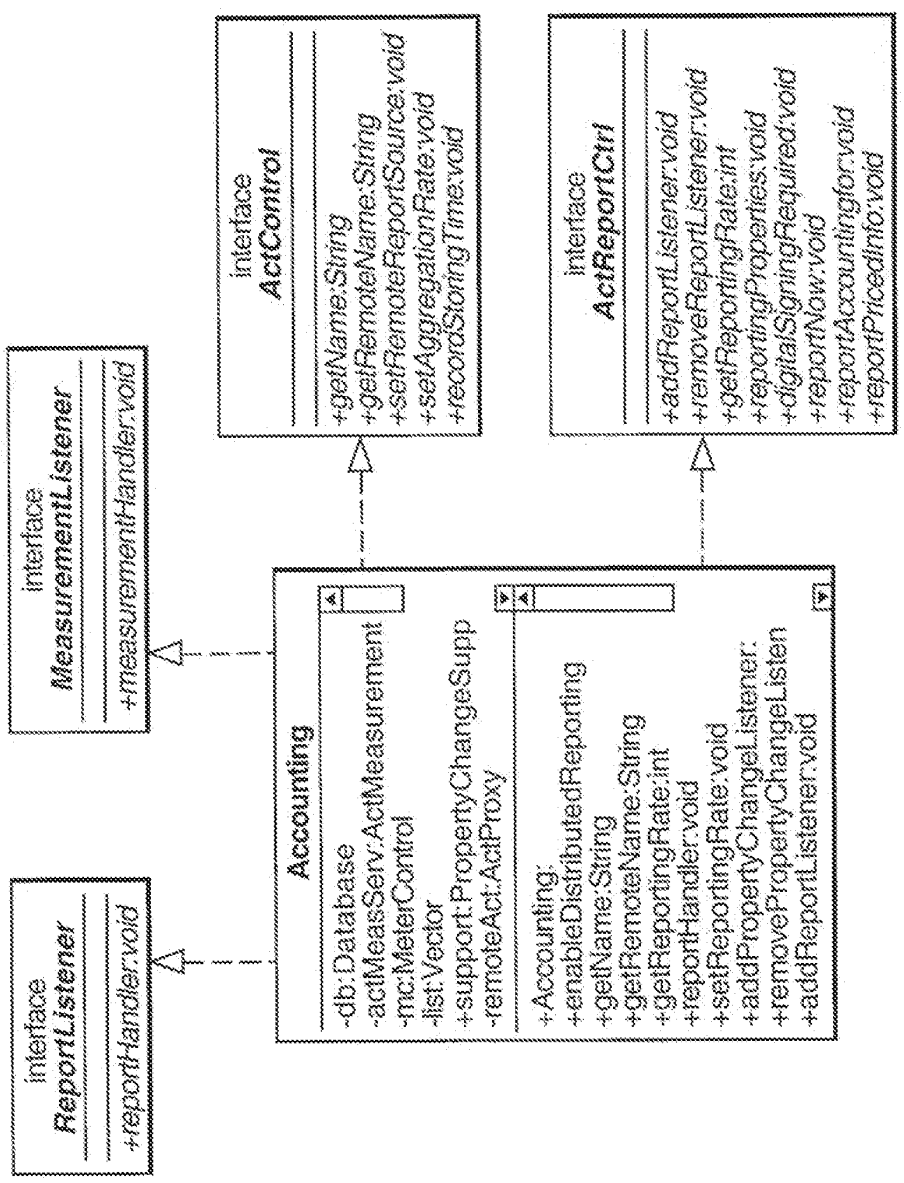

interface
ReportListener
+reportHandler:void
interface
MeasurementListener
+measurementHandler:void
Accounting
-db:Database
-actMeasServ:ActMeasurement
-mc:MeterControl
-list:Vector
+support:PropertyChangeSupp
-remoteAct:ActProxy
+Accounting:
+enableDistributedReporting
+getName:String
+getRemoteName:String
+getReportingRate:int
+reportHandler:void
+setReportingRate:void
+addPropertyChangeListener:
+removePropertyChangeListen
+addReportListener:void
interface
ActControl
+getName:String
+getRemoteName:String
+setRemoteReportSource:void
+setAggregationRate:void
+recordStoringTime:void
interface
ActReportCtrl
+actdReportListener:void
+removeReportListener:void
+getReportingRate:int
+reportingProperties:void
+digitalSigningRequired:void
+reportNow:void
+reportAccountingfor:void
+reportPricedInfo:void

Fig.8b.

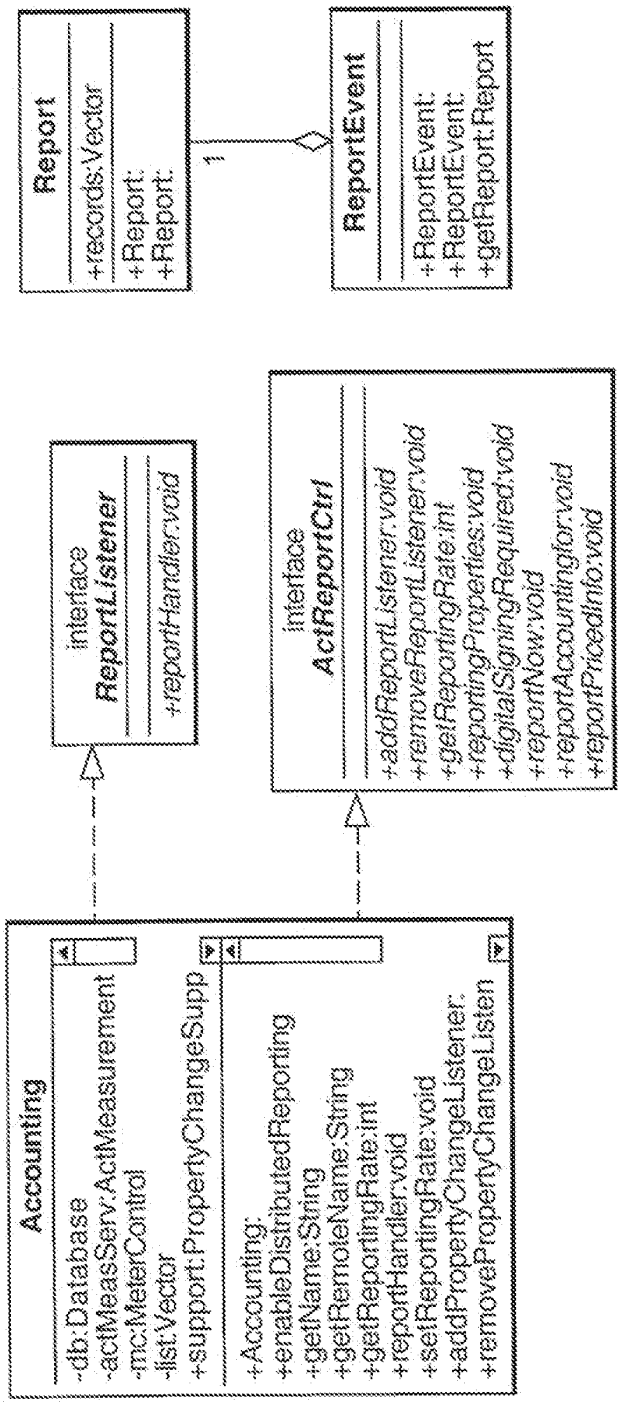

Report
+records:Vector
+Report:
+Report:
1
ReportEvent
+ReportEvent:
+ReportEvent:
+getReport:Report
interface
ReportListener
+reportHandler:void
interface
ActReportCtrl
+addReportListener:void
+removeReportListener:void
+getReportingRate:int
+reportingProperties:void
+digitalSigningRequired:void
+reportNow:void
+reportAccountingFor:void
+reportProceedInfo:void
Accounting
-db:Database
-actMeasServ:ActMeasurement
-mcMeterControl
-listVector
+supportPropertyChangeSupp
+Accounting:
+enableDistributedReporting
+getName:String
+getRemoteName:String
+getReportingRate:int
+reportHandler:void
+setReportingRate:void
+addPropertyChangeListener:
+removePropertyChangeListen

Fig.8c.

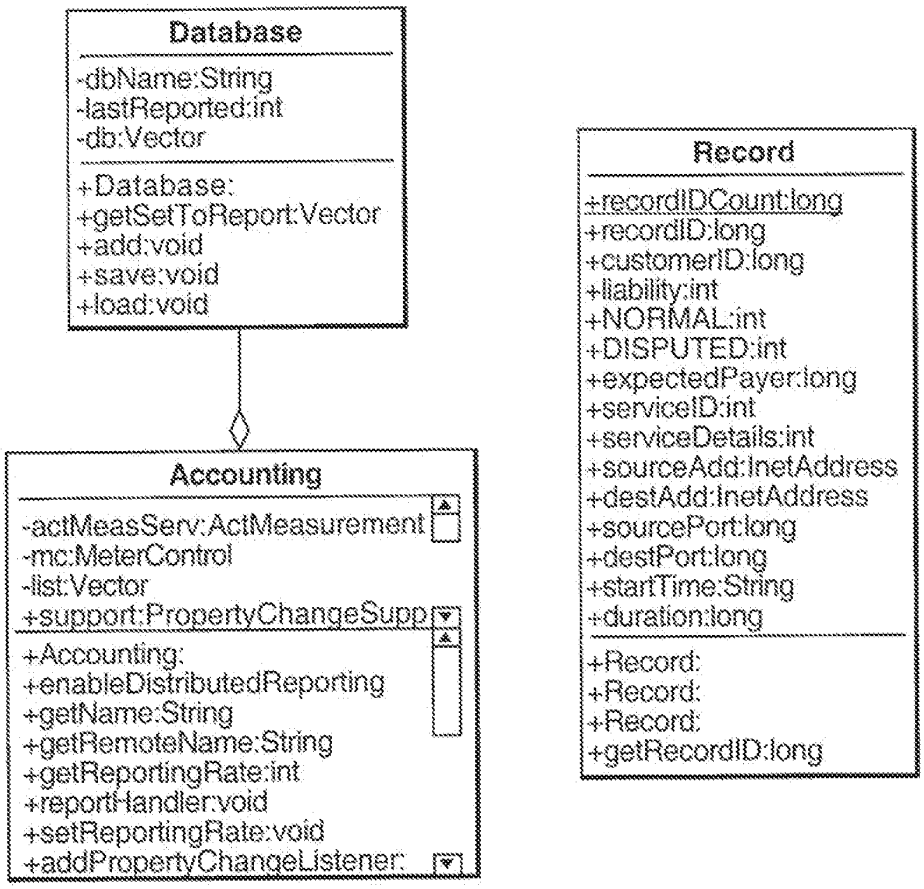

Database
-dbName:String
-lastReported:int
-db:Vector
+Database:
+getSetToReport:Vector
+add:void
+save:void
+load:void
Record
+recordIDCount:long
+recordID:long
+customerID:long
+liability:int
+NORMAL:int
+DISPUTED:int
+expectedPayer:long
+serviceID:int
+serviceDetails:int
+sourceAdd:InetAddress
+destAdd:InetAddress
+sourcePort:long
+destPort:long
+startTime:String
+duration:long
+Record:
+Record:
+Record:
+getRecordID:long
Accounting
-actMeasServ:ActMeasurement
-mc:MeterControl
-list:Vector
+support:PropertyChangeSupp
+Accounting:
+enableDistributedReporting
+getName:String
+getRemoteName:String
+getReportingRate:int
+reportHandler:void
+setReportingRate:void
+addPropertyChangeListener:

Fig.8d.

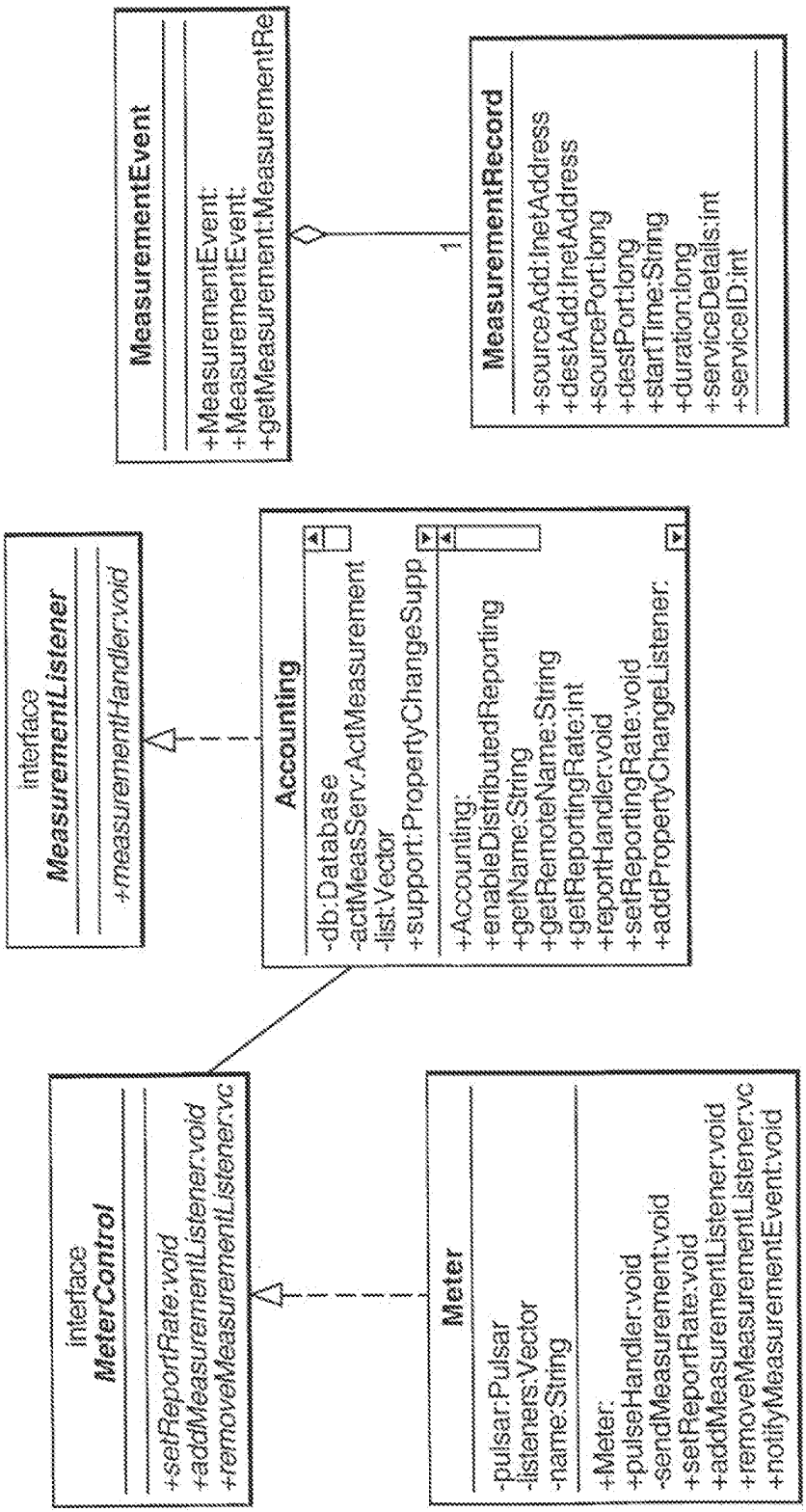

interface
MeasurementListener
+measurementHandler:void
Accounting
-db:Database
-actMeasServ:ActMeasurement
-list:Vector
+support:PropertyChangeSupp
+Accounting:
+enableDistributedReporting
+getName:String
+getRemoteName:String
+getReportingRate:int
+reportHandler:void
+setReportingRate:void
+addPropertyChangeListener:
MeasurementEvent
+MeasurementEvent:
+MeasurementEvent:
+getMeasurement:MeasurementRe
1
MeasurementRecord
+sourceAdd:InetAddress
+destAdd:InetAddress
+sourcePort:long
+destPort:long
+startTime:String
+duration:long
+serviceDetails:int
+serviceID:int
interface
MeterControl
+setReportRate:void
+addMeasurementListener:void
+removeMeasurementListener:vc
Meter
-pulsar:Pulsar
-listeners:Vector
-name:String
+Meter:
+pulseHandler:void
-sendMeasurement:void
+setReportRate:void
+addMeasurementListener:void
+removeMeasurementListener:vc
+notifyMeasurementEvent:void

Fig.8e.

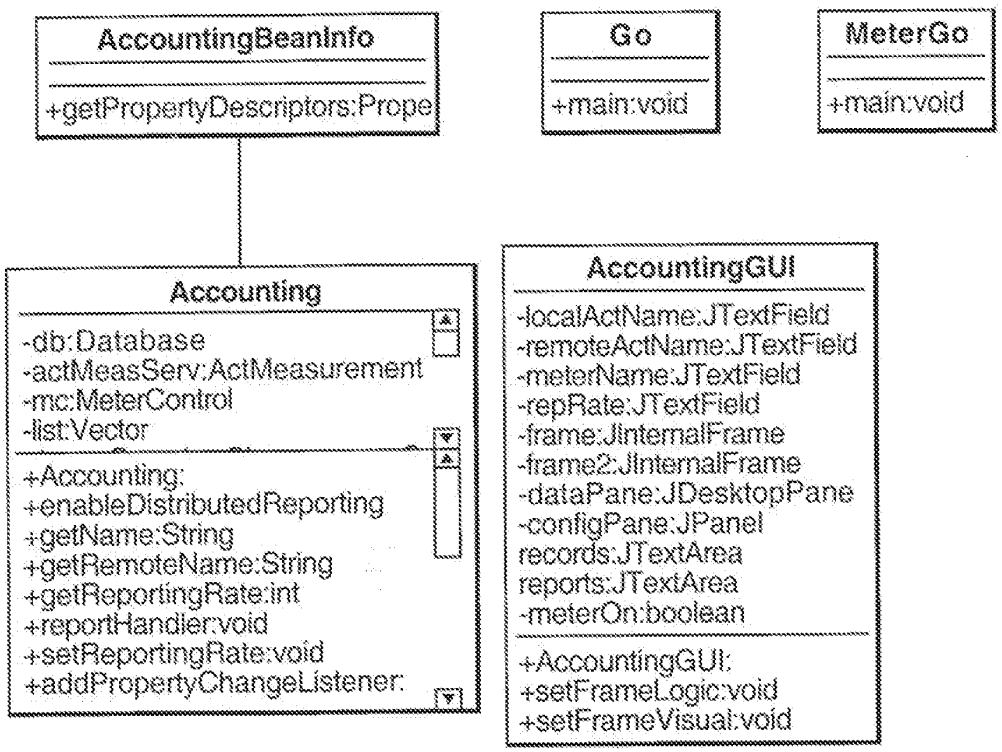

AccountingBeanInfo
+getPropertyDescriptors:Prope
Go
+main:void
MeterGo
+main:void
Accounting
-db:Database
-actMeasServ:ActMeasurement
-mc:MeterControl
-list:Vector
+Accounting:
+enableDistributedReporting
+getName:String
+getRemoteName:String
+getReportingRate:int
+reportHandler:void
+setReportingRate:void
+addPropertyChangeListener:
AccountingGUI
-localActName:JTextField
-remoteActName:JTextField
-meterName:JTextField
-repRate:JTextField
-frame:JInternalFrame
-frame2:JInternalFrame
-dataPane:JDesktopPane
-configPane:JPanel
records:JTextArea
reports:JTextArea
-meterOn:boolean
+AccountingGUI:
+setFrameLogic:void
+setFrameVisual:void

Fig.9.

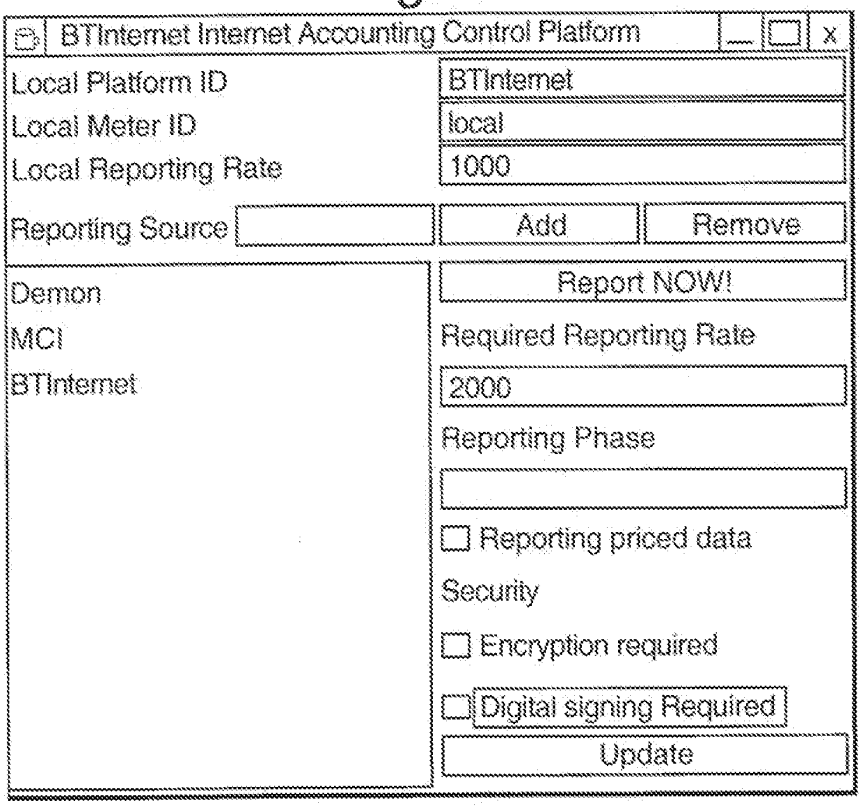

BTInternet Internet Accounting Control Platform
Local Platform ID
BTInternet
Local Meter ID
local
Local Reporting Rate
1000
Reporting Source
Add
Remove
Demon
MCI
BTInternet
Report NOW!
Required Reporting Rate
2000
Reporting Phase
Reporting priced data
Security
Encryption required
Digital signing Required
Update

Fig.10.

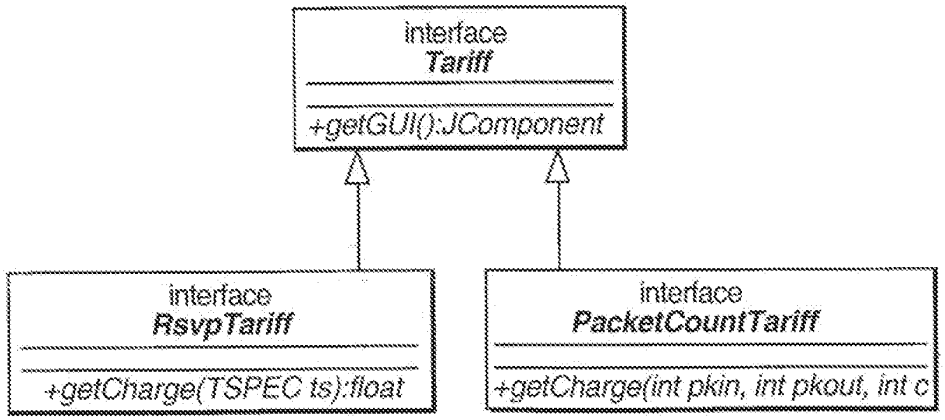
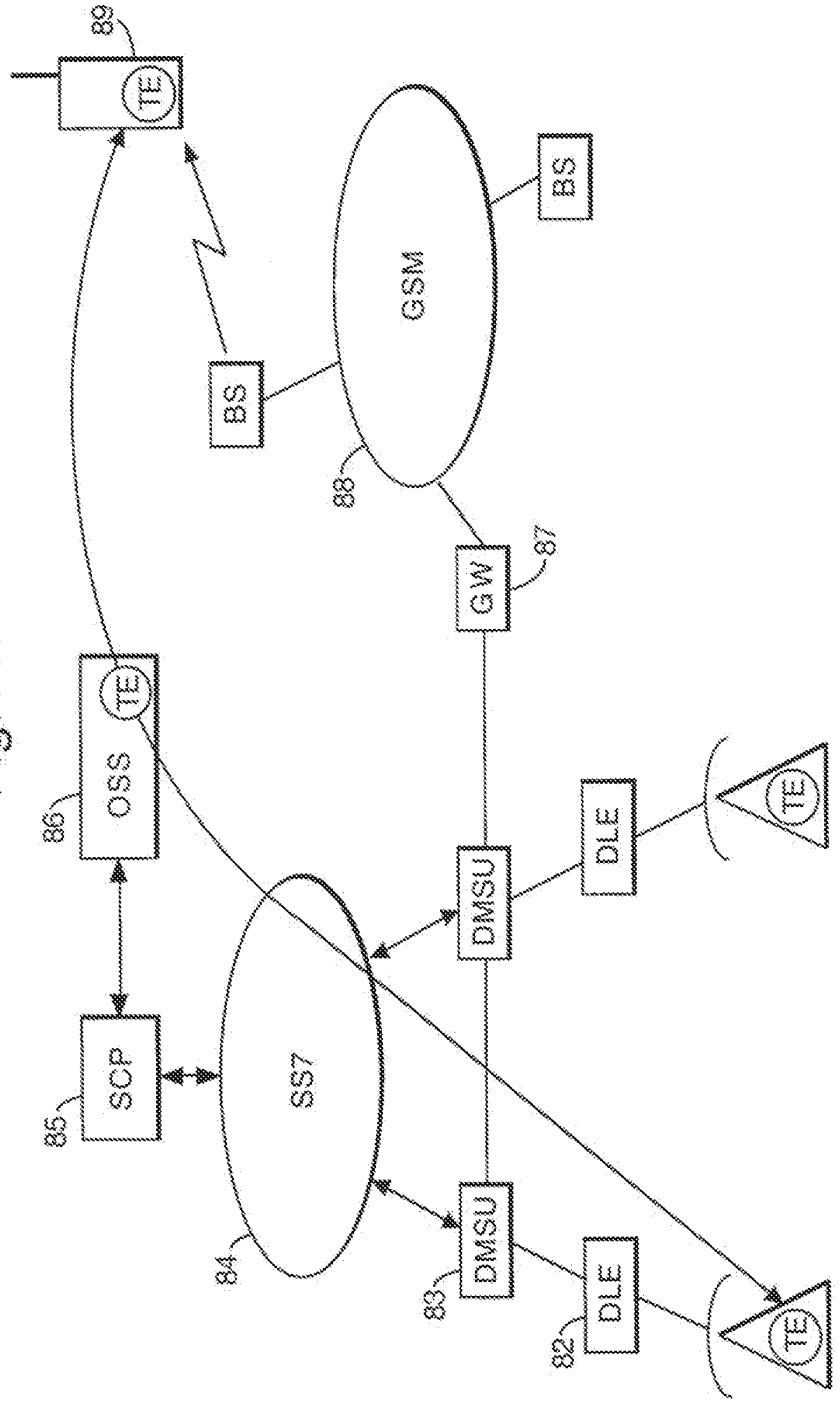

interface
Tariff
+getGUI():JComponent
interface
RsvpTariff
+getCharge(TSPEC ts):float
interface
PacketCountTariff
+getCharge(int pkin, int pkout, int c

Fig.11.


89
TE
BS
GSM
BS
88
GW
87
OSS
TE
86
DMSU
DLE
TE
SCP
85
SS7
84
DMSU
83
DLE
82
TE

# Electronic Acknowledgement Receipt

| | |
|---|---|
| **EFS ID:** | 8297985 |
| **Application Number:** | 12694445 |
| **International Application Number:** | |
| **Confirmation Number:** | 6030 |
| **Title of Invention:** | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES |
| **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:** | RALEP025 |
| **Receipt Date:** | 27-AUG-2010 |
| **Filing Date:** | 27-JAN-2010 |
| **Time Stamp:** | 16:08:39 |
| **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 | RALEP025_IDS_Before_1st_OA.pdf | 56034<br>b36609e32bb1573319e137a68cec19f5bb392ab0 | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | Information Disclosure Statement (IDS) Filed (SB/08) | RALEP025_IDS_SB08_3.pdf | 87659<br>6068edf65380488bf2a6eefe1475e0ad65bc54cd | no | 1 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| This is not an USPTO supplied IDS fillable form | | | | | |
| 3 | Foreign Reference | RALE_Foreign_Ref_3A.pdf | 7292666<br>bda2da57ab175aa54d24e9cd7699784789063e0a | no | 55 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 4 | Foreign Reference | RALE_Foreign_Ref_3B.pdf | 4238695<br>2b1ac857c7db7ca12f5a92190a59fb4eac5e537a | no | 29 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 5 | NPL Documents | RALE_NPL_Ref_3C.pdf | 117093<br>adaccc6f7b2b7c7891095a31e01c2a5c2182ad86 | no | 8 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 6 | NPL Documents | RALE_NPL_Ref_3D.pdf | 1817585<br>1b0cb7a0b41b1340ba9e48fa0ea77e27f1632f33 | no | 10 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 7 | NPL Documents | RALE_NPL_Ref_3E.pdf | 184255<br>2e2daf80298dda3e93323c4a7f91f1ec3e478c42 | no | 9 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 8 | NPL Documents | RALE_NPL_Ref_3F.pdf | 5141787<br>6ecd30cfa00263c87082d7274ae16e8caa198bf1 | no | 35 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 9 | NPL Documents | RALE_NPL_Ref_3G.pdf | 1451509<br>e95282786ba86e4a05ee8c793a9ec634aa5a654c | no | 6 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 10 | NPL Documents | RALE_NPL_Ref_3H.pdf | 128010<br>8d35d15d27cc8636c1526980a75aa6a4a97a745d | no | 9 |

| | | | | | |
|---|---|---|---|---|---|
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 11 | NPL Documents | RALE_NPL_Ref_3I.pdf | 112089<br>24c595d8153db4b6ba795d5be64c6f98b0573749 | no | 5 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 12 | NPL Documents | RALE_NPL_Ref_3J.pdf | 338617<br>74671591bbc19ab5364956f70d29b176cce30b1f | no | 11 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 13 | NPL Documents | RALE_NPL_Ref_3K.pdf | 2587996<br>104930755650d3cb8fbbb63837dc7338fbc2bd3c | no | 16 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 14 | NPL Documents | RALE_NPL_Ref_3L.pdf | 1050612<br>c5435588dd68fcddc7835e4dce1e6489894a398b | no | 124 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 15 | Foreign Reference | RALE_Foreign_Ref_3M.pdf | 6080065<br>c95895297c2769217788ac8dce979a79e9d20d33 | no | 49 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| | | **Total Files Size (in bytes):** | 30684672 | | |

**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.: | 12/694,445 | Art Unit: | 2614 |
| Filed: | January 27, 2010 | Docket No.: | RALEP025 |
| Title: | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | | |

## 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. RALEP025).

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.: | 12/694,445 |
| | | | | Filing Date | January 27, 2010 |
| | | | | First Named Inventor | Gregory G. Raleigh |
| | | | | Art Unit | 2614 |
| | | | | Examiner Name | Not Assigned |
| Sheet | 1 | of | 2 | Atty Docket No. | RALEP025 |

| 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 | |
| | | | |

PTO/SB/08 (08-03)

| Substitute for form 1449/PTO | | | | *Complete if Known* | |
|---|---|---|---|---|---|
| **Information Disclosure Statement By Applicant** *(Use as many sheets as necessary)* | | | | Application No.: | 12/694,445 |
| | | | | Filing Date | January 27, 2010 |
| | | | | First Named Inventor | Gregory G. Raleigh |
| | | | | Art Unit | 2614 |
| | | | | Examiner Name | Not Assigned |
| Sheet | 2 | of | 2 | Atty Docket No. | RALEP025 |

| | | | |
|---|---|---|---|
| | | | |

| 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

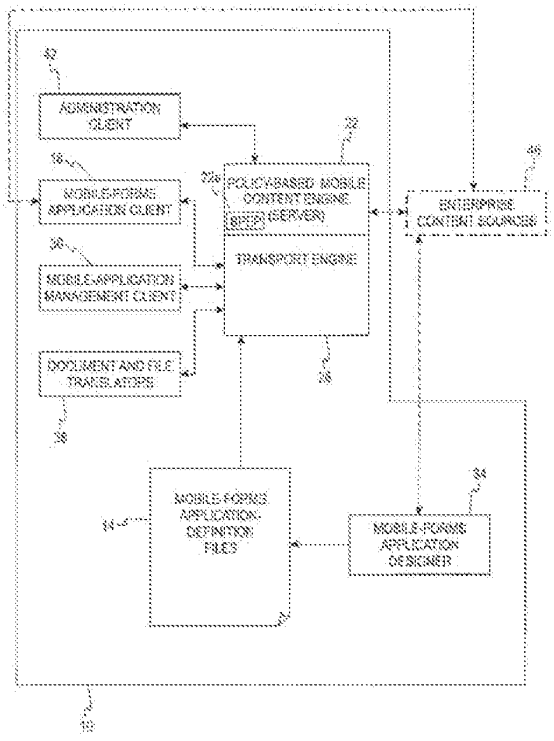
(75) Inventors/Applicants *(for US only)*: **CHANE, Marc** [CA/CA]; 111-29 Main Street, Ottawa, Ontario K1S 1B1 (CA). **MCGUIRE, Kevin** [CA/CA]; 41 Wimbledon Way, Ottawa, Ontario K2E 3J2 (CA). **PEYTON, Liam** [CA/CA]; 767 Rolling River Crescent, Ottawa, Ontario K1V 1M2 (CA).

(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, Alova, 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.

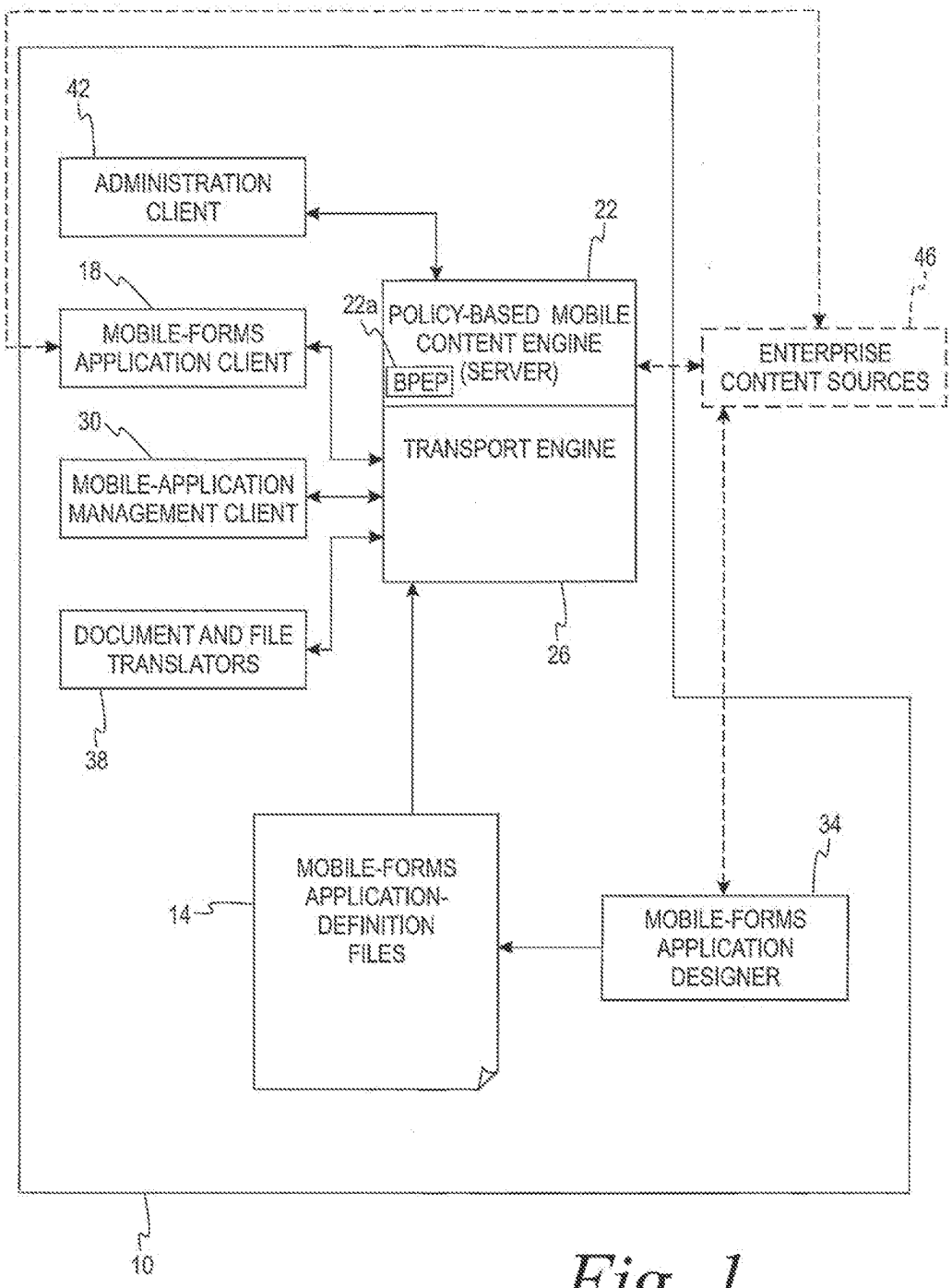

42
ADMINISTRATION CLIENT
22
46
18
22a
POLICY-BASED MOBILE CONTENT ENGINE
BPEP
(SERVER)
MOBILE-FORMS APPLICATION CLIENT
ENTERPRISE CONTENT SOURCES
30
TRANSPORT ENGINE
MOBILE-APPLICATION MANAGEMENT CLIENT
DOCUMENT AND FILE TRANSLATORS
26
38
34
MOBILE-FORMS APPLICATION-DEFINITION FILES
14
MOBILE-FORMS APPLICATION DESIGNER
10

*Fig. 1*

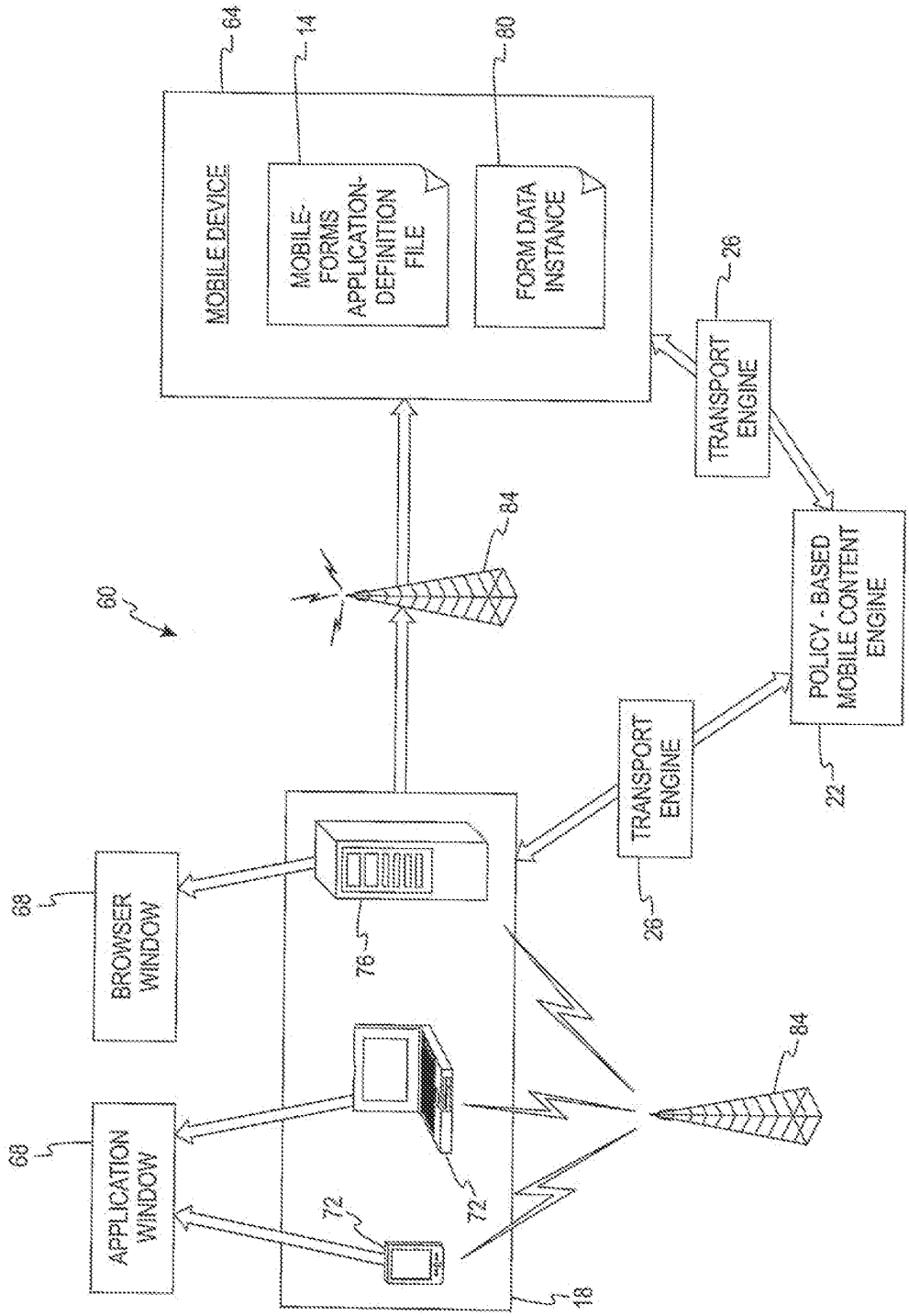

64
14
80
MOBILE DEVICE
MOBILE-FORMS APPLICATION-DEFINITION FILE
FORM DATA INSTANCE
26
TRANSPORT ENGINE
POLICY - BASED MOBILE CONTENT ENGINE
22
TRANSPORT ENGINE
28
84
60
68
BROWSER WINDOW
76
68
APPLICATION WINDOW
72
72
18

*Fig. 2*

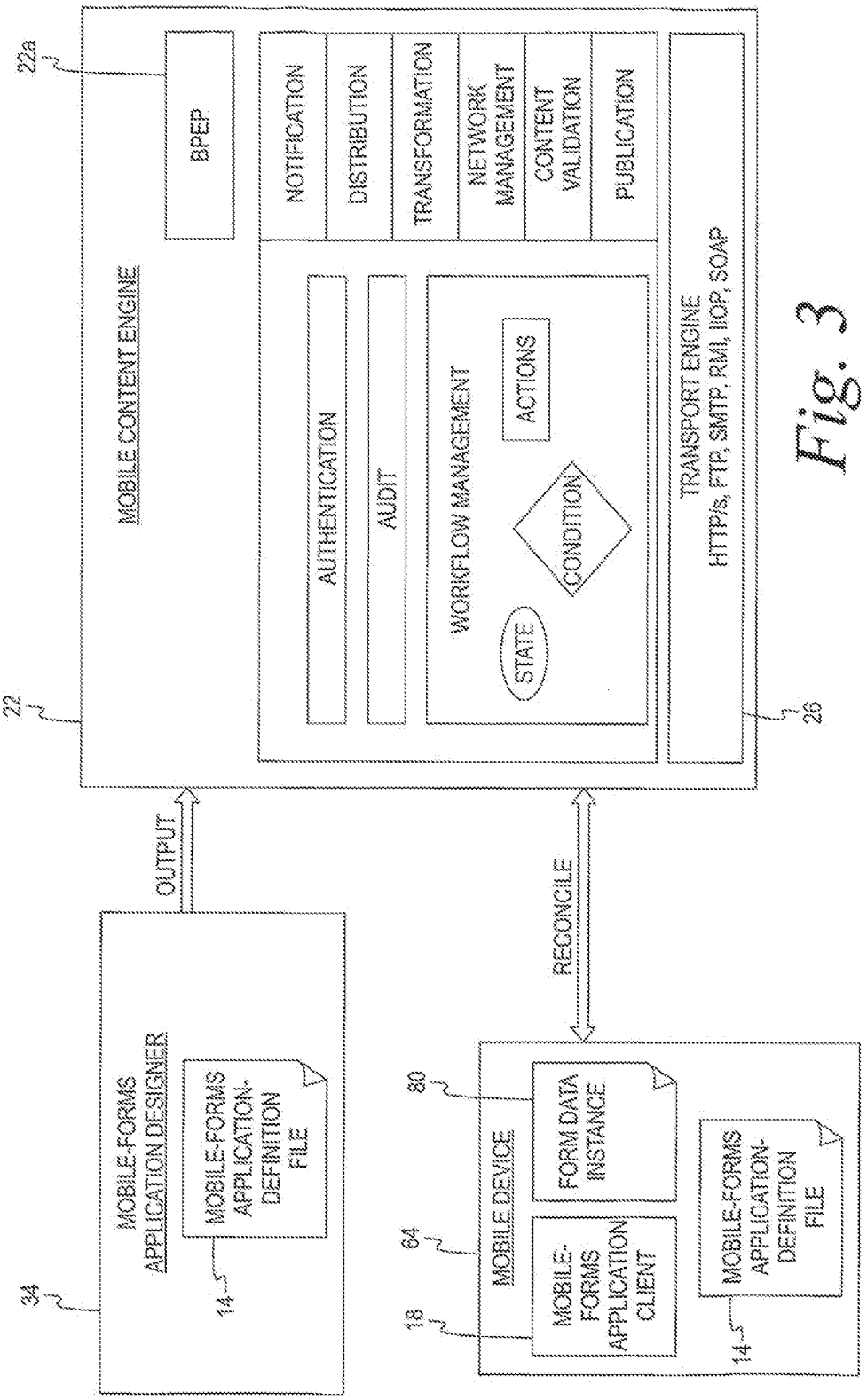

22a
MOBILE CONTENT ENGINE
BPEP
NOTIFICATION
DISTRIBUTION
TRANSFORMATION
NETWORK MANAGEMENT
CONTENT VALIDATION
PUBLICATION
AUTHENTICATION
AUDIT
WORKFLOW MANAGEMENT
ACTIONS
CONDITION
STATE
TRANSPORT ENGINE
HTTP/s, FTP, SMTP, RMI, IIOP, SOAP
22
26
OUTPUT
RECONCILE
MOBILE-FORMS APPLICATION DESIGNER
MOBILE-FORMS APPLICATION-DEFINITION FILE
34
14
80
64
18
MOBILE DEVICE
FORM DATA INSTANCE
MOBILE-FORMS APPLICATION CLIENT
MOBILE-FORMS APPLICATION-DEFINITION FILE
14

*Fig. 3*

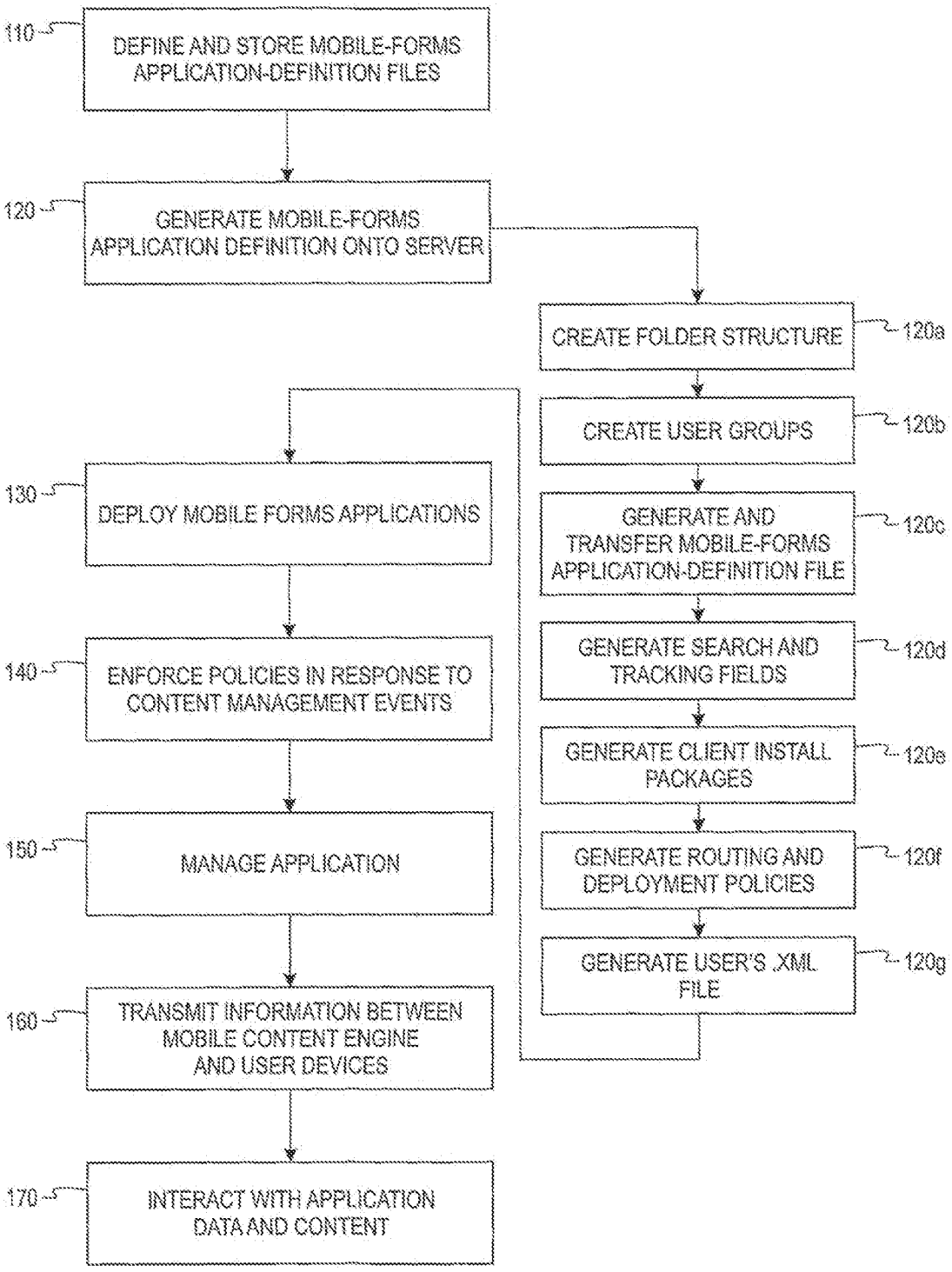

110
DEFINE AND STORE MOBILE-FORMS APPLICATION-DEFINITION FILES
120
GENERATE MOBILE-FORMS APPLICATION DEFINITION ONTO SERVER
CREATE FOLDER STRUCTURE
120a
CREATE USER GROUPS
120b
GENERATE AND TRANSFER MOBILE-FORMS APPLICATION-DEFINITION FILE
120c
GENERATE SEARCH AND TRACKING FIELDS
120d
GENERATE CLIENT 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)<br>see whole document | 1-34 |
| Y | US 2003/0220879 (Gaughan et al.) 27 November 2003 (27-11-2003)<br>see whole document | 1-30 |
| Y | US 5,034,096 (Beizer) 01 October 1991 (01-10-1991)<br>see whole document | 31-34 |
| A | WO 01/61517 (Buisman et al.) 23 August 2001 (23-08-2001)<br>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<br>Place du Portage I, C114 - 1st Floor, Box PCT<br>50 Victoria Street<br>Gatineau, Quebec K1A 0C9<br>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

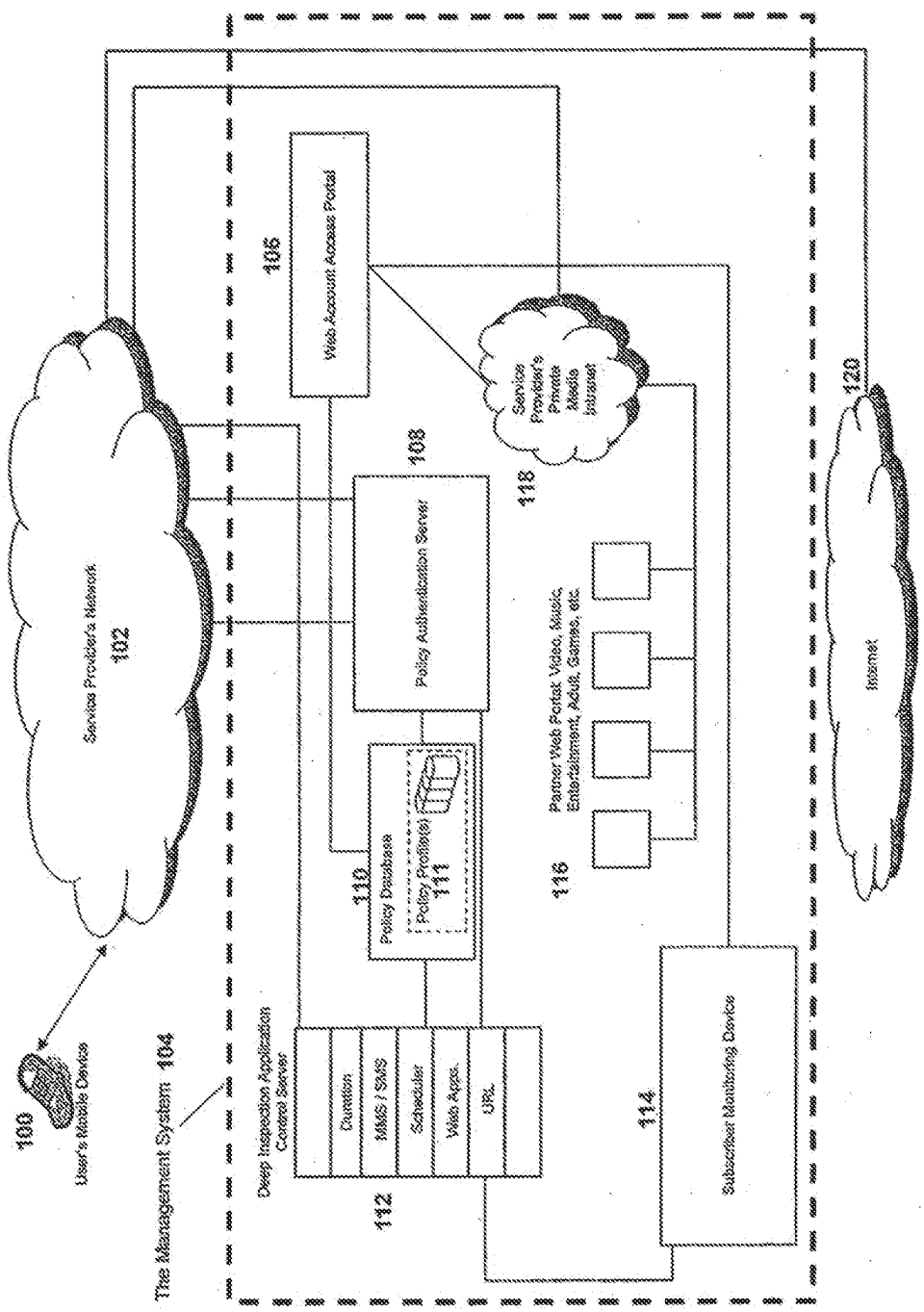

100
User's Mobile Device
Service Provider's Network
102
The Management System 104
Deep Inspection Application Control Server
Duration
MMS / SMS
Scheduler
Web Apps
URL
112
Policy Database
Policy Profile(s)
111
110
Policy Authentication Server
108
Web Account Access Portal
106
Service Provider's Private Media Intranet
118
Partner Web Portal: Video, Music, Entertainment, Adult, Games, etc.
116
Subscriber Monitoring Device
114
Internet
120

Fig. 2

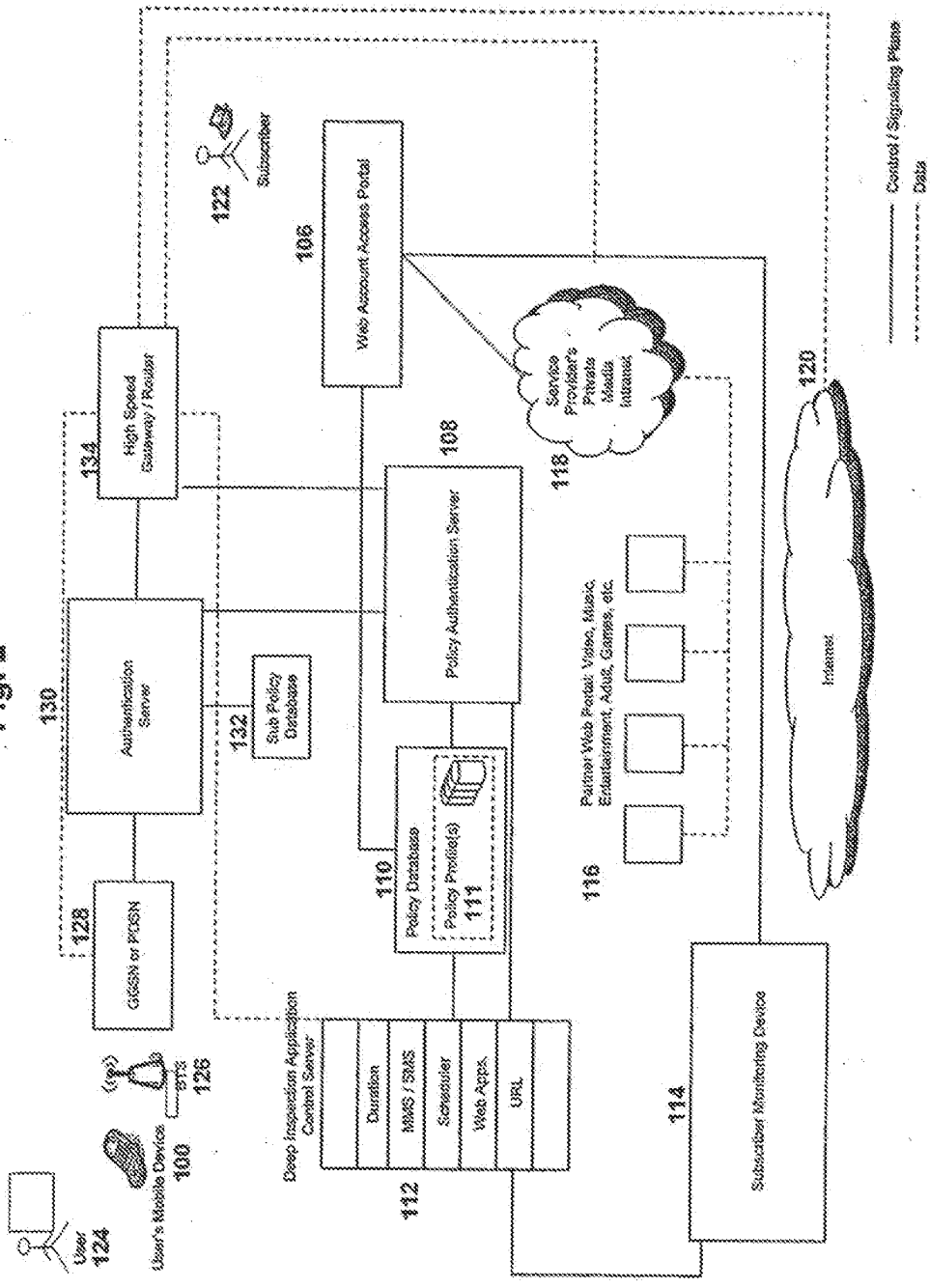

Control / Signaling Plane
Data
Subscriber
122
Web Account Access Portal
106
High Speed Gateway / Router
134
Service Provider's Private Media Intranet
118
120
Internet
Policy Authentication Server
108
Authentication Server
130
Sub Policy Database
132
Partner Web Portal: Video, Music, Entertainment, Adult, Games, etc.
116
Policy Database
110
Policy Profile(s)
111
GSM/GPRS or PDSN
128
Deep Inspection Application Control Server
Duration
MMS / SMS
Screensaver
Web Apps
URL
112
Subscriber Monitoring Device
114
User's Mobile Device
100
126
User
124

Fig. 3

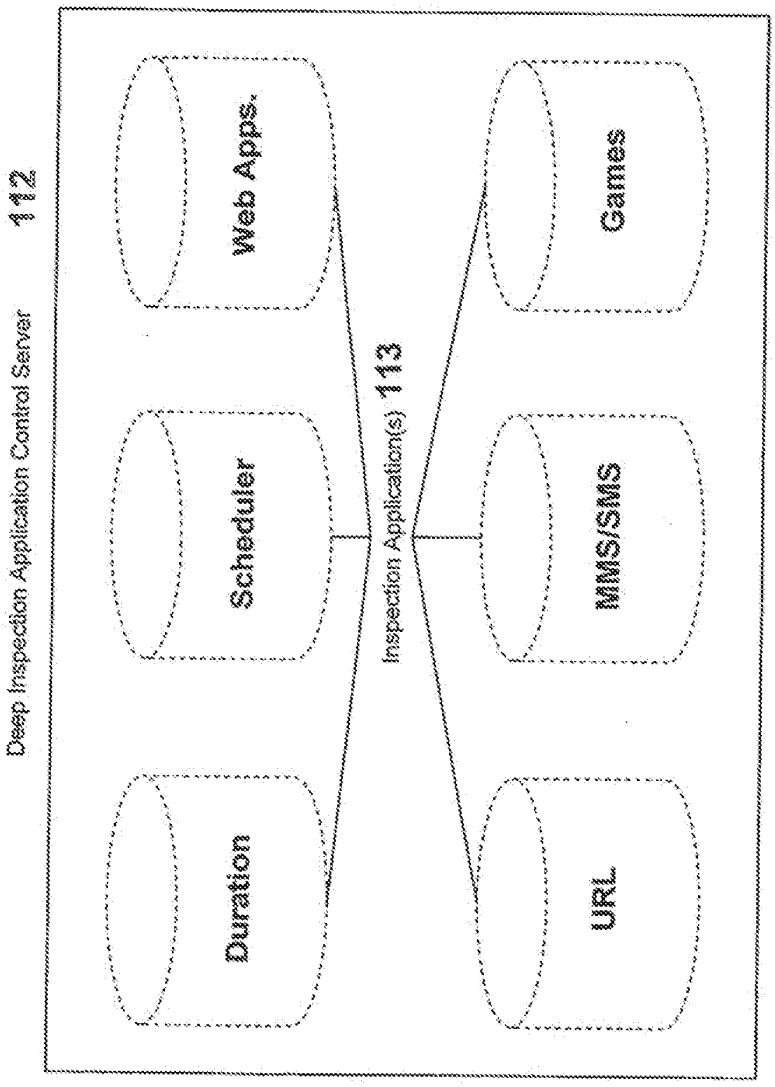
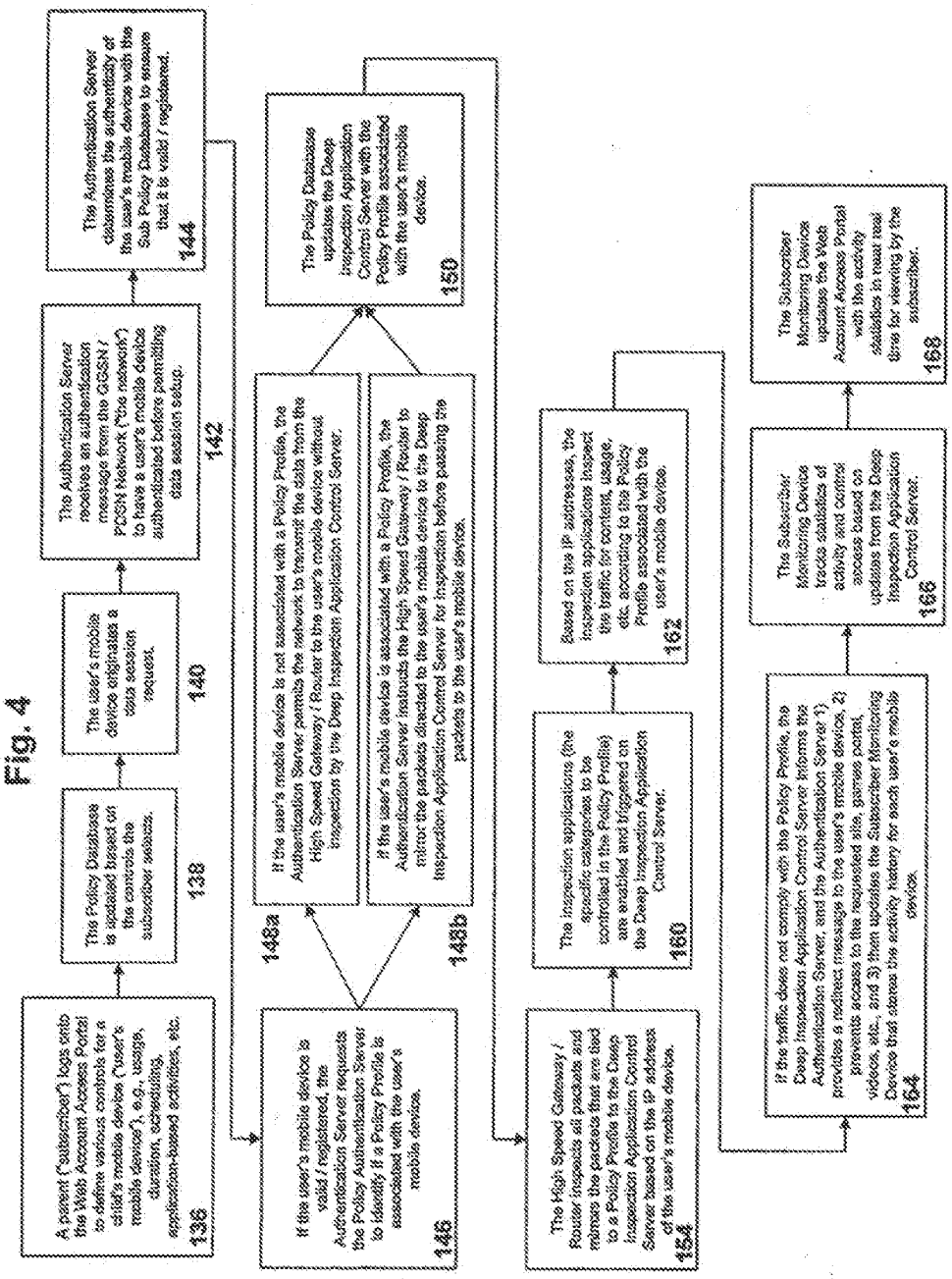

Deep Inspection Application Control Server 112
Inspection Application(s) 113
Web Apps.
Scheduler
Duration
Games
MMS/SMS
URL

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
This 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 ensure that it is valid / registered.
144
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
148a
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.
148b
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.
150
The Policy Database updates the Deep Inspection Application Control Server with the Policy Profile associated with the user's mobile device.
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).

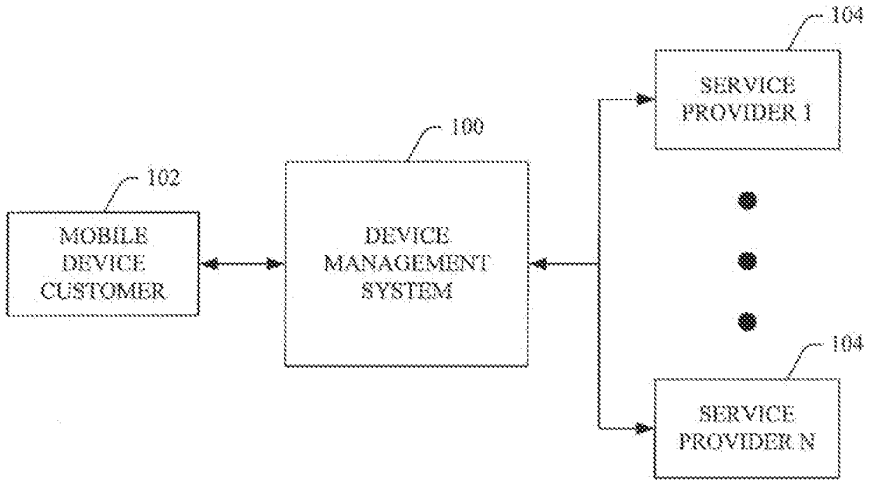
(74) Agents: **DORTENZO, Megan D.** et al.; Thompson Hine LLP, 127 Public Square, 3900 Key Center, Cleveland, OH 44114 (US).

(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.

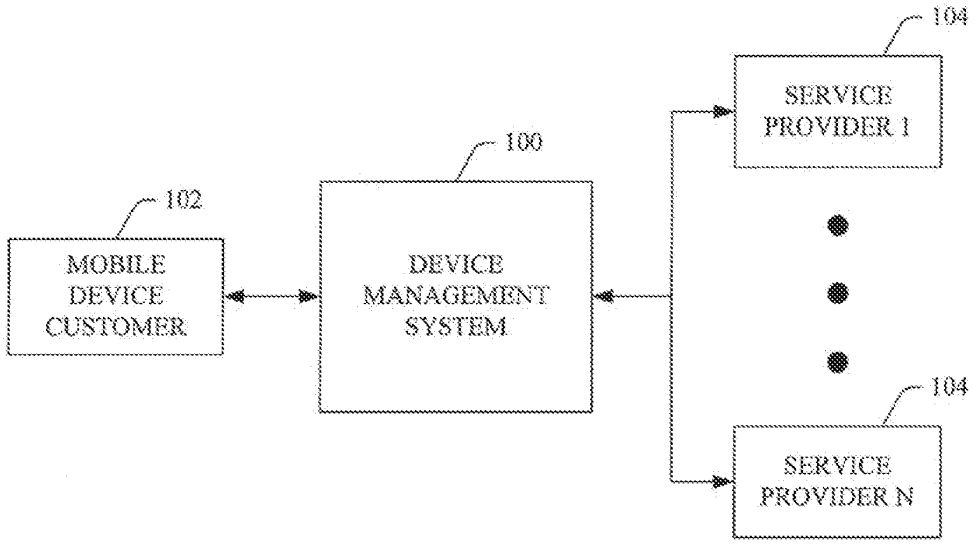

104
SERVICE PROVIDER 1
100
102
MOBILE DEVICE CUSTOMER
DEVICE MANAGEMENT SYSTEM
104
SERVICE PROVIDER N

FIG. 1

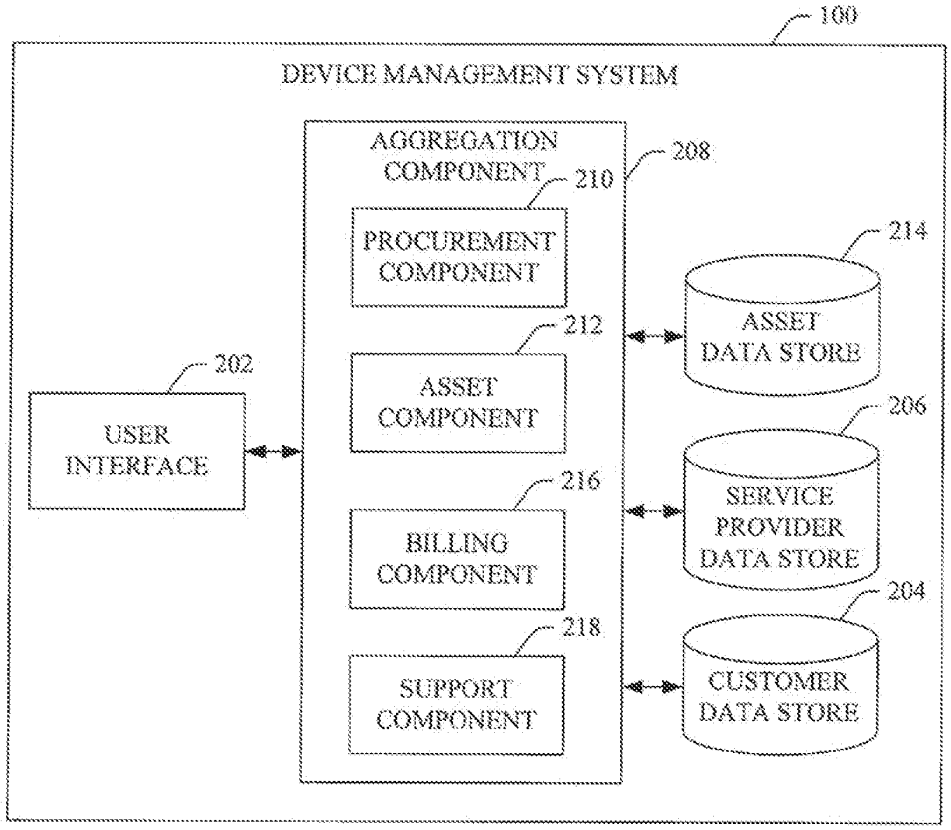

100
DEVICE MANAGEMENT SYSTEM
AGGREGATION COMPONENT
208
210
PROCUREMENT COMPONENT
212
ASSET COMPONENT
216
BILLING COMPONENT
218
SUPPORT COMPONENT
202
USER INTERFACE
214
ASSET DATA STORE
206
SERVICE PROVIDER DATA STORE
204
CUSTOMER DATA STORE

FIG. 2

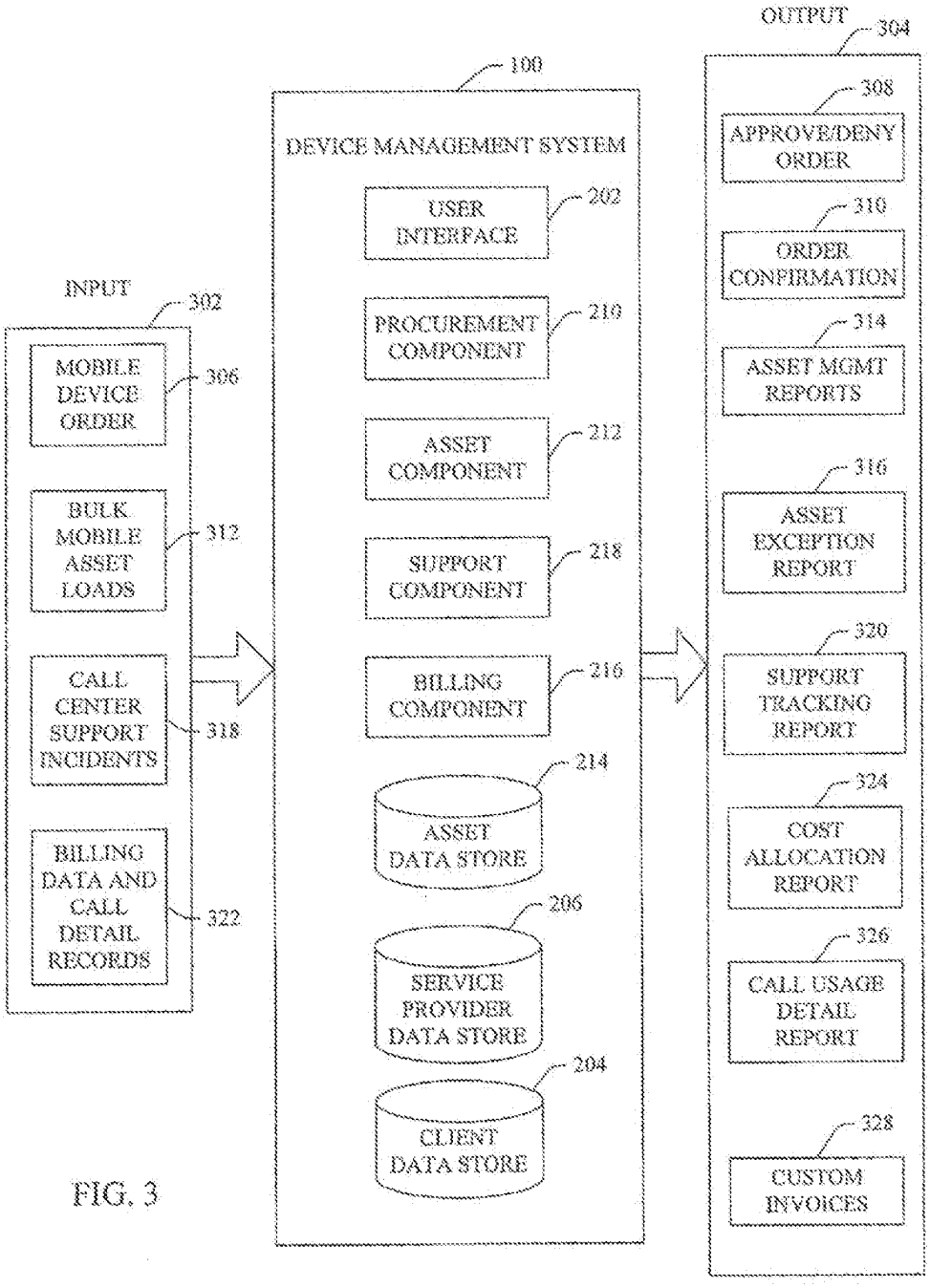

INPUT
302
MOBILE DEVICE ORDER
306
BULK MOBILE ASSET LOADS
312
CALL CENTER SUPPORT INCIDENTS
318
BILLING DATA AND CALL DETAIL RECORDS
322
100
DEVICE MANAGEMENT SYSTEM
USER INTERFACE
202
PROCUREMENT COMPONENT
210
ASSET COMPONENT
212
SUPPORT COMPONENT
218
BILLING COMPONENT
216
ASSET DATA STORE
214
SERVICE 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

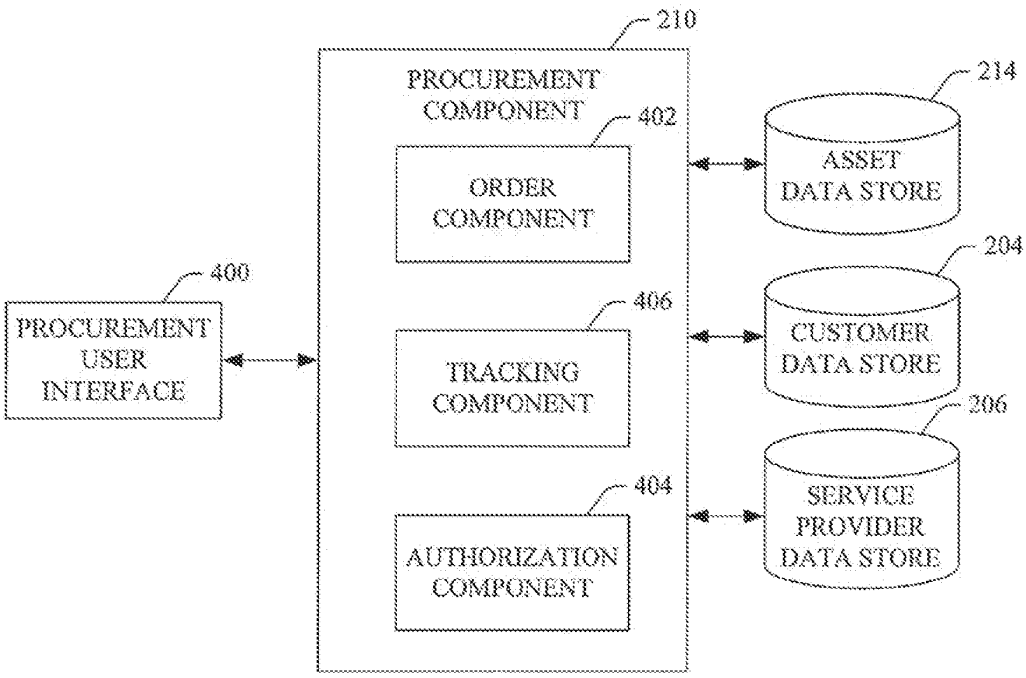

210
PROCUREMENT COMPONENT
402
ORDER COMPONENT
406
TRACKING COMPONENT
404
AUTHORIZATION COMPONENT
400
PROCUREMENT USER INTERFACE
214
ASSET DATA STORE
204
CUSTOMER DATA STORE
206
SERVICE PROVIDER DATA STORE

FIG. 4

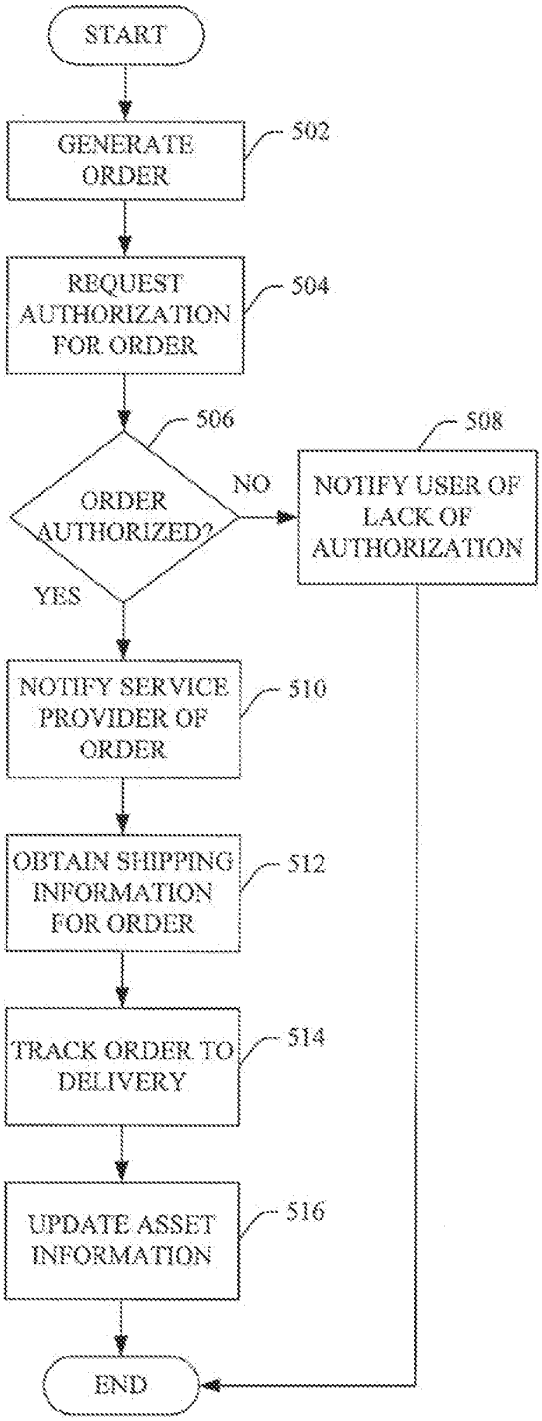

START
GENERATE ORDER
502
REQUEST AUTHORIZATION FOR ORDER
504
506
ORDER AUTHORIZED?
NO
508
NOTIFY USER OF LACK OF AUTHORIZATION
YES
NOTIFY SERVICE PROVIDER OF ORDER
510
OBTAIN SHIPPING INFORMATION FOR ORDER
512
TRACK ORDER TO DELIVERY
514
UPDATE ASSET INFORMATION
516
END

FIG. 5

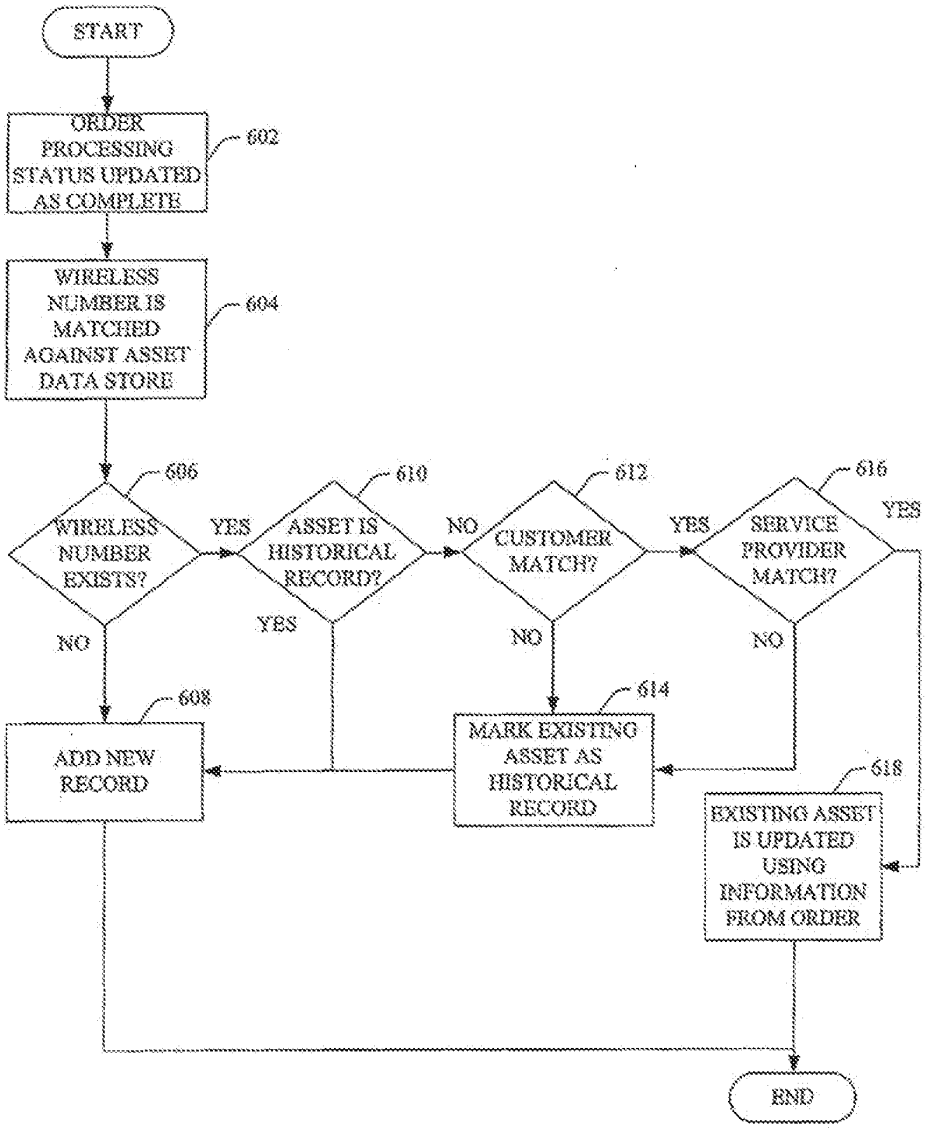

START
ORDER PROCESSING STATUS UPDATED AS COMPLETE
602
WIRELESS NUMBER IS MATCHED AGAINST ASSET DATA STORE
604
606
WIRELESS NUMBER EXISTS?
YES
610
ASSET IS HISTORICAL RECORD?
NO
612
CUSTOMER MATCH?
YES
616
SERVICE PROVIDER MATCH?
YES
NO
YES
NO
NO
608
ADD NEW RECORD
614
MARK EXISTING ASSET AS HISTORICAL RECORD
618
EXISTING ASSET IS UPDATED USING INFORMATION FROM ORDER
END

FIG. 6

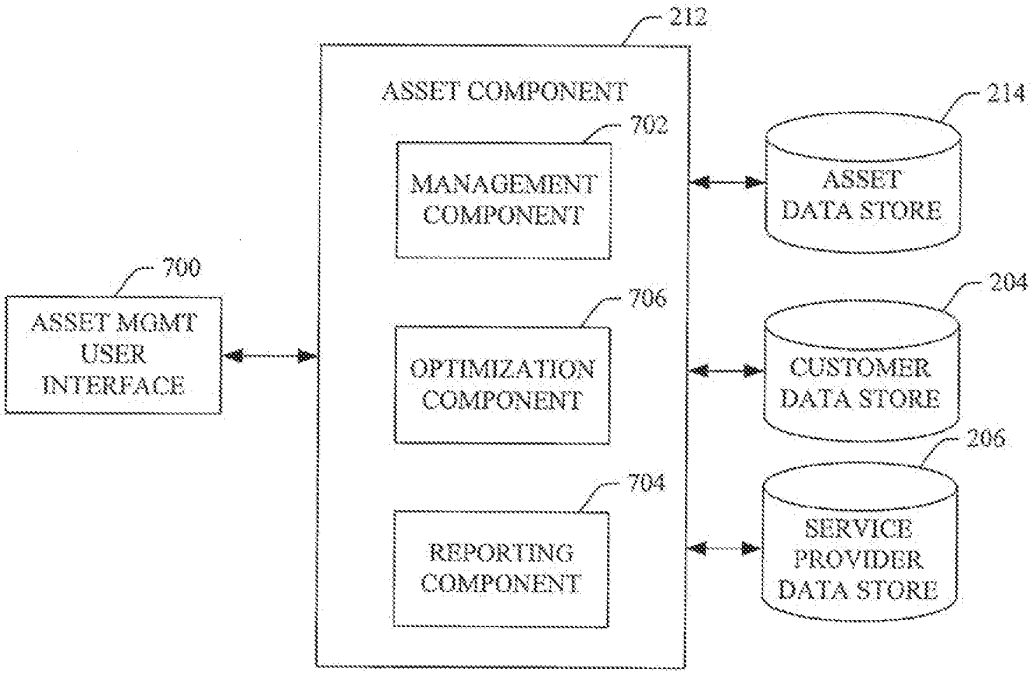

212
ASSET COMPONENT
702
MANAGEMENT COMPONENT
706
OPTIMIZATION COMPONENT
704
REPORTING COMPONENT
214
ASSET DATA STORE
204
CUSTOMER DATA STORE
206
SERVICE PROVIDER DATA STORE
700
ASSET MGMT USER INTERFACE

FIG. 7

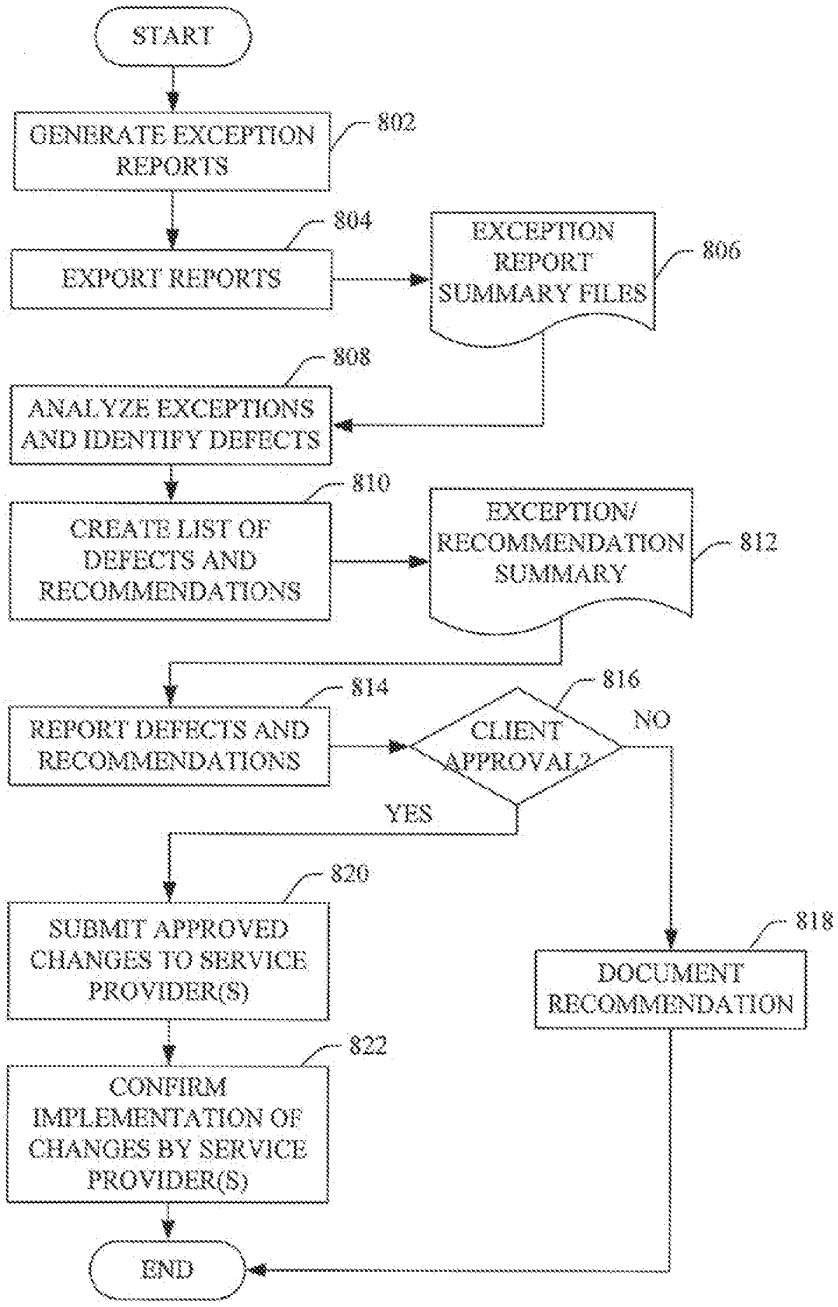

START
GENERATE EXCEPTION REPORTS
802
EXPORT REPORTS
804
EXCEPTION REPORT SUMMARY FILES
806
ANALYZE EXCEPTIONS AND IDENTIFY DEFECTS
808
CREATE LIST OF DEFECTS AND RECOMMENDATIONS
810
EXCEPTION/ RECOMMENDATION SUMMARY
812
REPORT DEFECTS AND RECOMMENDATIONS
814
CLIENT APPROVAL?
816
NO
YES
SUBMIT APPROVED CHANGES TO SERVICE PROVIDER(S)
820
DOCUMENT RECOMMENDATION
818
CONFIRM IMPLEMENTATION OF CHANGES BY SERVICE PROVIDER(S)
822
END

FIG. 8

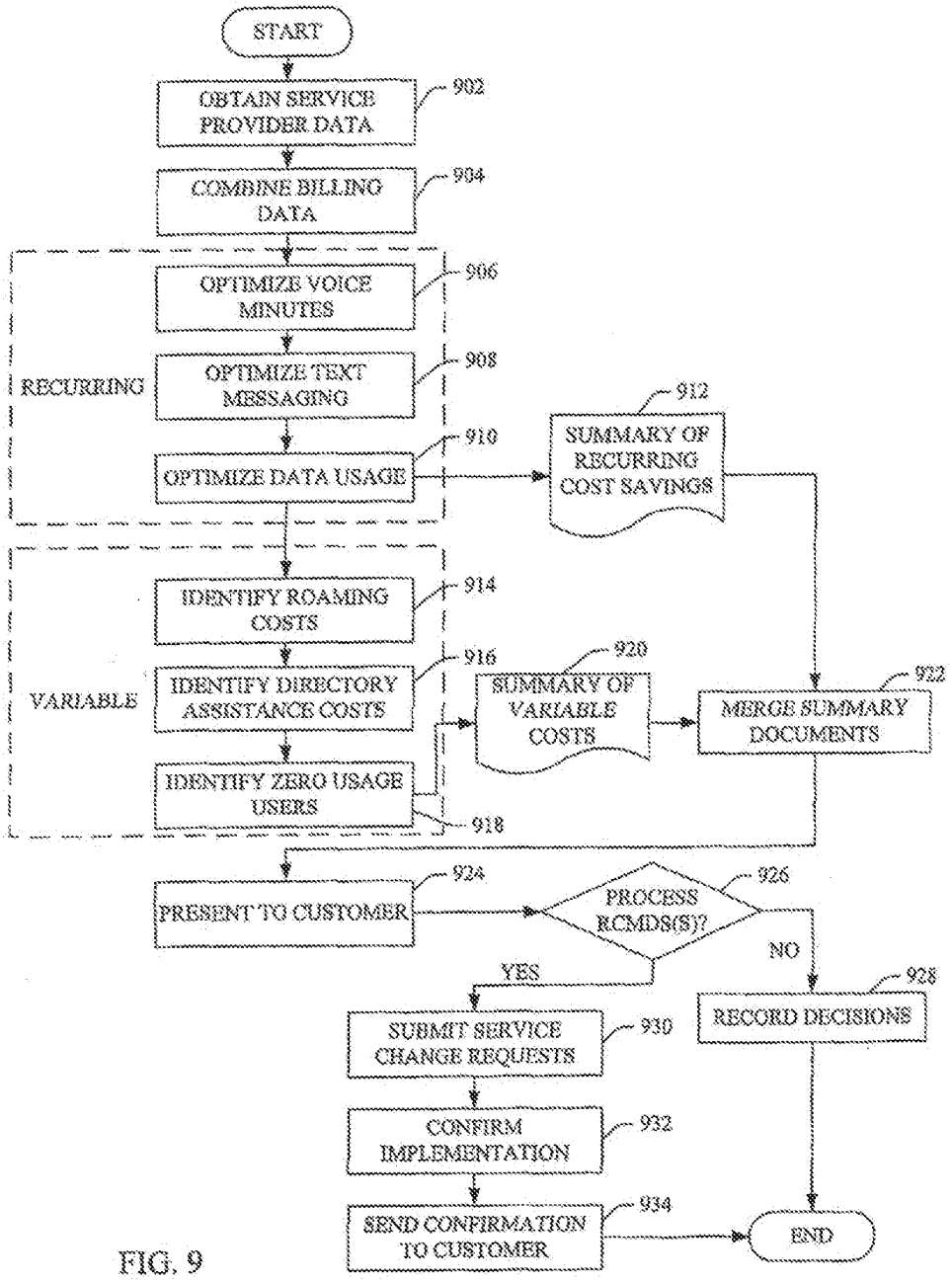

START
OBTAIN SERVICE PROVIDER DATA
902
COMBINE BILLING DATA
904
RECURRING
OPTIMIZE VOICE MINUTES
906
OPTIMIZE TEXT MESSAGING
908
OPTIMIZE DATA USAGE
910
SUMMARY OF RECURRING COST SAVINGS
912
VARIABLE
IDENTIFY ROAMING COSTS
914
IDENTIFY DIRECTORY ASSISTANCE COSTS
916
IDENTIFY ZERO USAGE USERS
918
SUMMARY 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

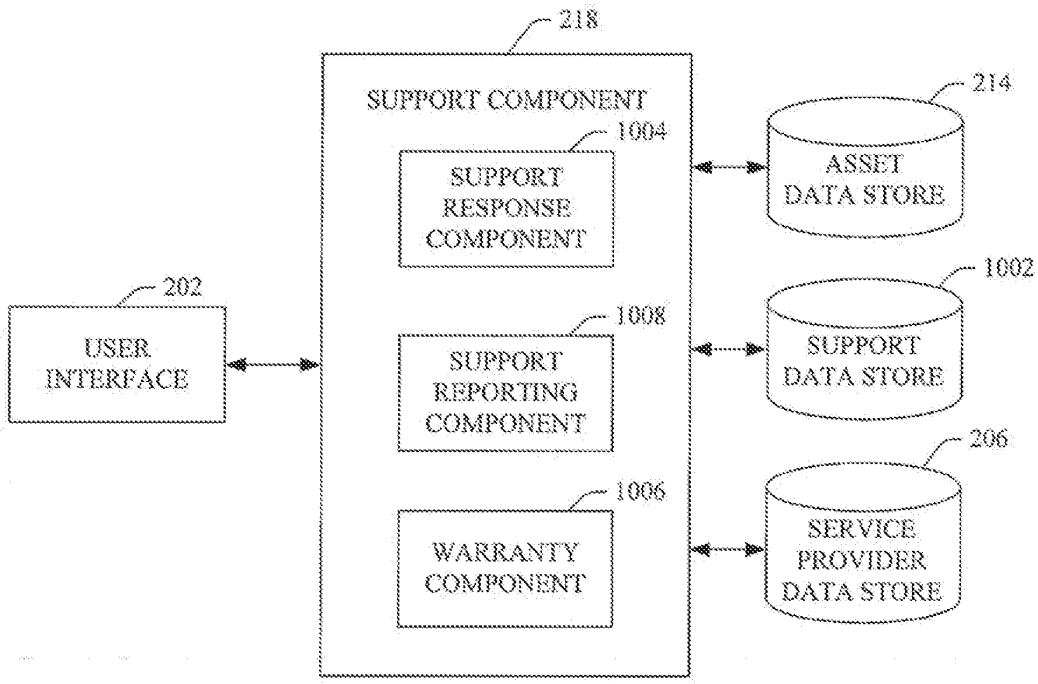

218
SUPPORT COMPONENT
1004
SUPPORT RESPONSE COMPONENT
1008
SUPPORT REPORTING COMPONENT
1006
WARRANTY COMPONENT
202
USER INTERFACE
214
ASSET DATA STORE
1002
SUPPORT DATA STORE
206
SERVICE PROVIDER DATA STORE

FIG. 10

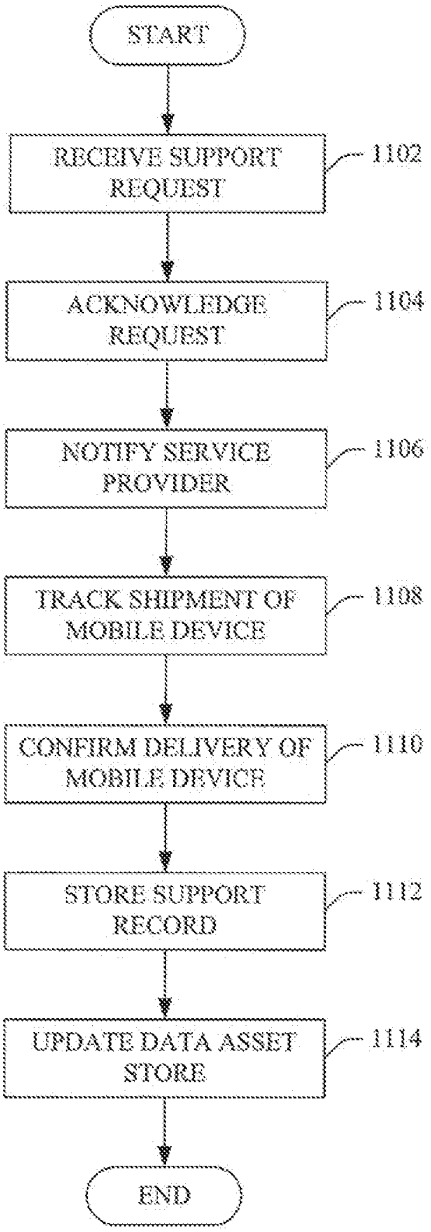

START
RECEIVE SUPPORT REQUEST
1102
ACKNOWLEDGE REQUEST
1104
NOTIFY SERVICE PROVIDER
1106
TRACK SHIPMENT OF MOBILE DEVICE
1108
CONFIRM DELIVERY OF MOBILE DEVICE
1110
STORE SUPPORT RECORD
1112
UPDATE DATA ASSET STORE
1114
END

FIG. 11

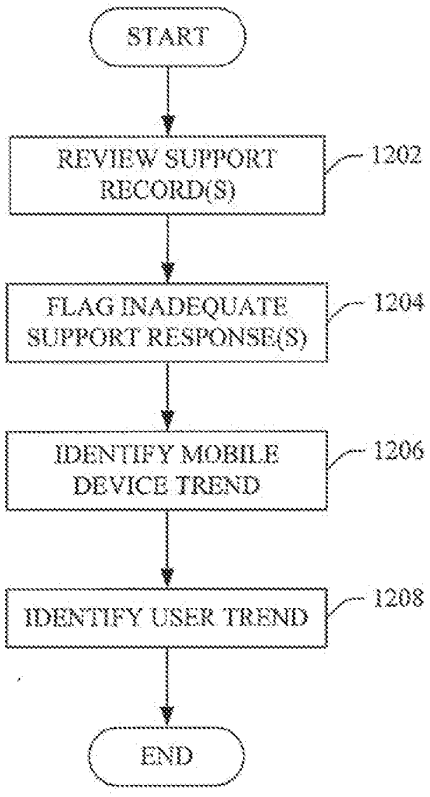

START
REVIEW SUPPORT RECORD(S)
1202
FLAG INADEQUATE SUPPORT RESPONSE(S)
1204
IDENTIFY MOBILE DEVICE TREND
1206
IDENTIFY USER TREND
1208
END

FIG. 12

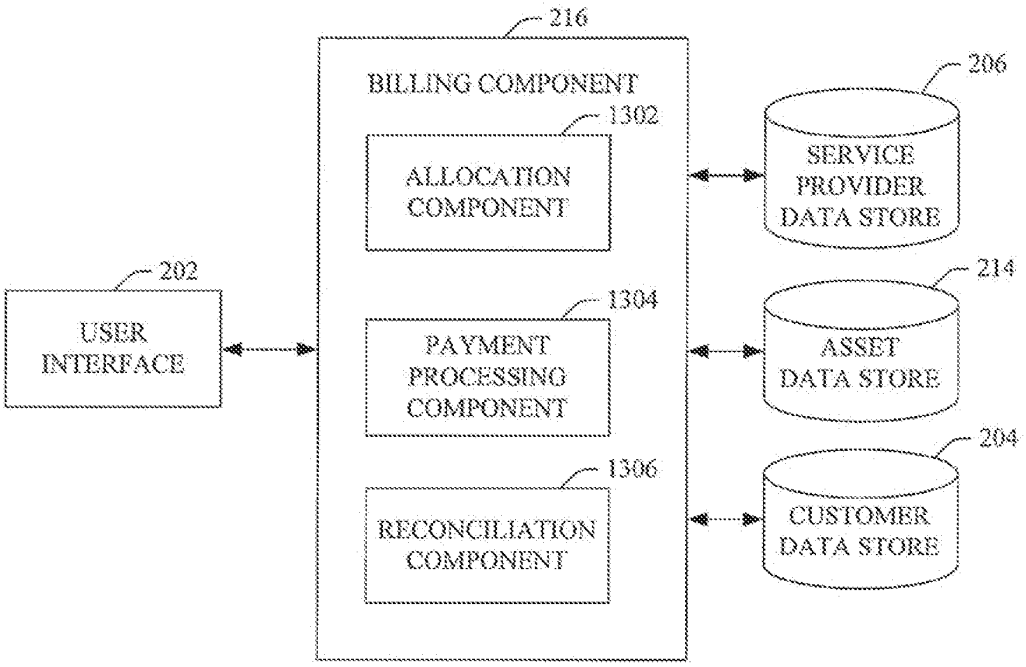

216
BILLING COMPONENT
1302
ALLOCATION COMPONENT
1304
PAYMENT PROCESSING COMPONENT
1306
RECONCILIATION COMPONENT
206
SERVICE PROVIDER DATA STORE
214
ASSET DATA STORE
204
CUSTOMER DATA STORE
202
USER INTERFACE

FIG. 13

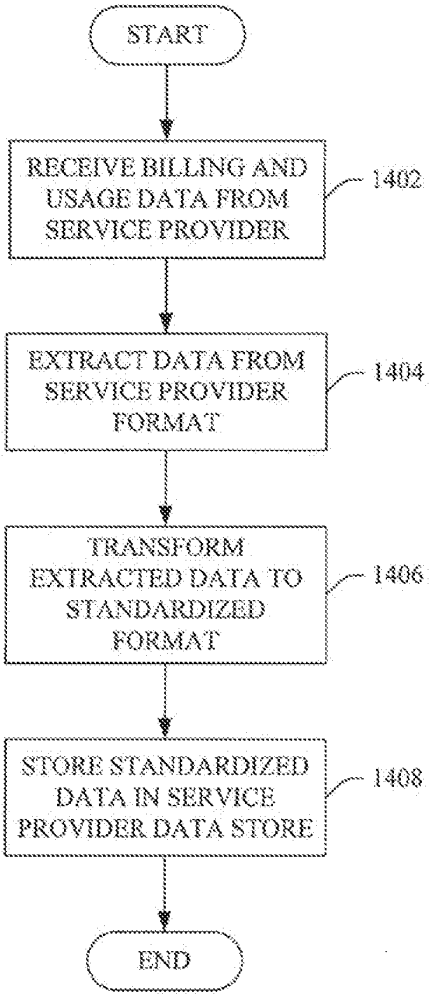

START
RECEIVE BILLING AND USAGE DATA FROM SERVICE PROVIDER
1402
EXTRACT DATA FROM SERVICE PROVIDER FORMAT
1404
TRANSFORM EXTRACTED DATA TO STANDARDIZED FORMAT
1406
STORE STANDARDIZED DATA IN SERVICE PROVIDER DATA STORE
1408
END

FIG. 14

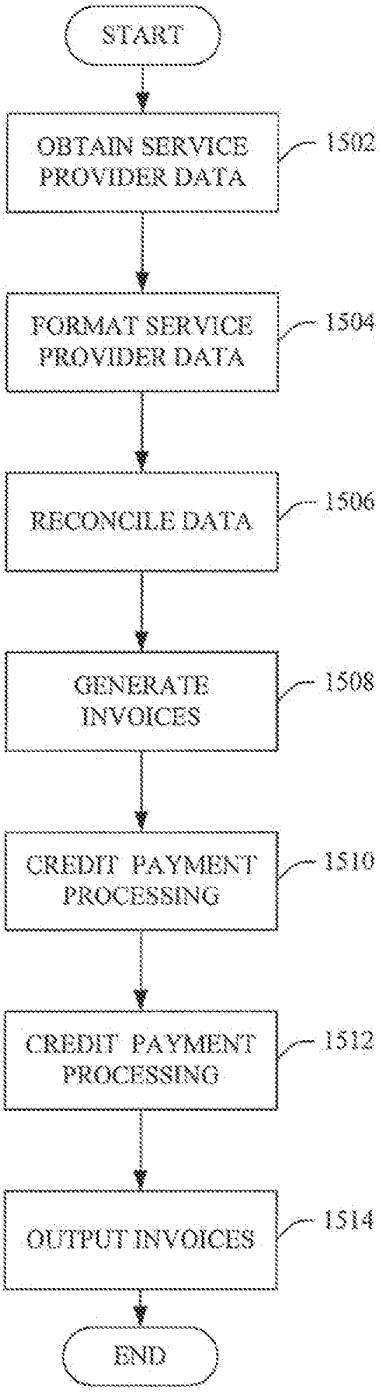

START
OBTAIN SERVICE PROVIDER DATA
1502
FORMAT SERVICE PROVIDER DATA
1504
RECONCILE DATA
1506
GENERATE INVOICES
1508
CREDIT PAYMENT PROCESSING
1510
CREDIT PAYMENT PROCESSING
1512
OUTPUT INVOICES
1514
END

FIG. 15

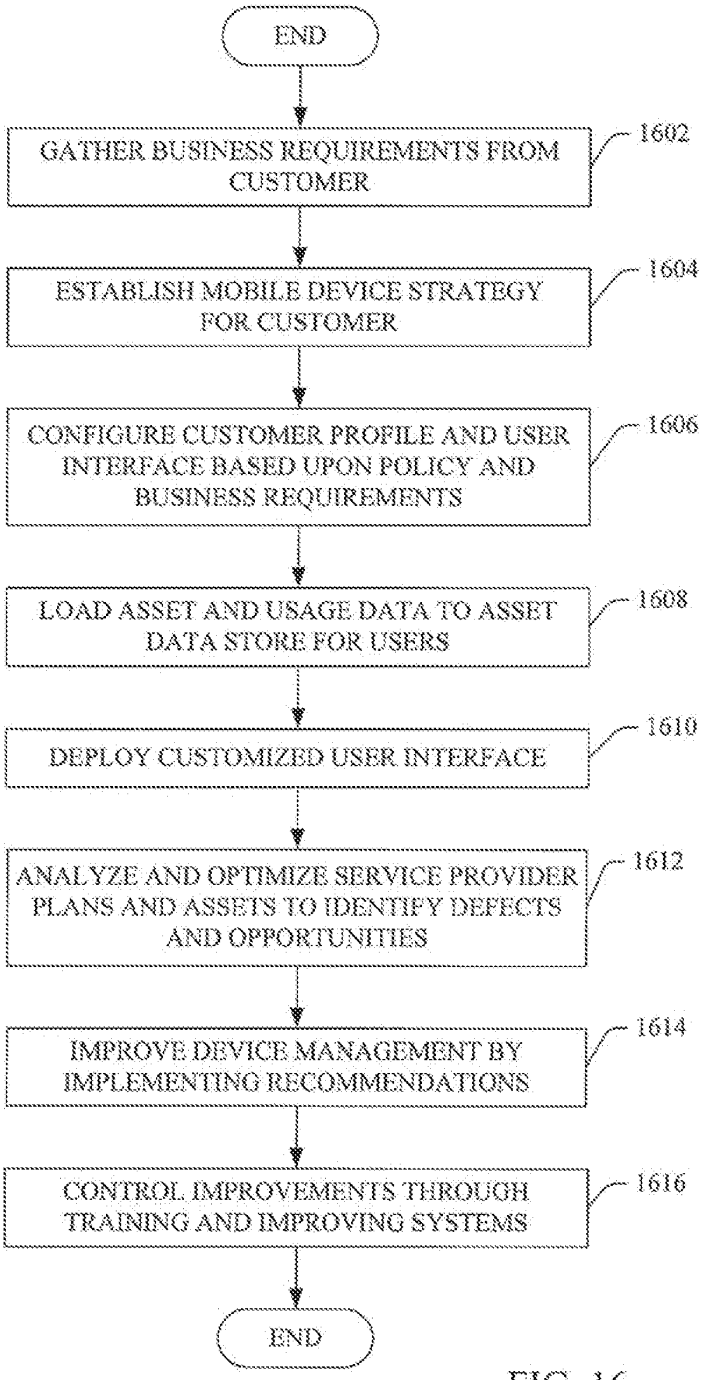

END
GATHER BUSINESS REQUIREMENTS FROM CUSTOMER
1602
ESTABLISH MOBILE DEVICE STRATEGY FOR CUSTOMER
1604
CONFIGURE CUSTOMER PROFILE AND USER INTERFACE BASED UPON POLICY AND BUSINESS REQUIREMENTS
1606
LOAD ASSET AND USAGE DATA TO ASSET DATA STORE FOR USERS
1608
DEPLOY CUSTOMIZED USER INTERFACE
1610
ANALYZE 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

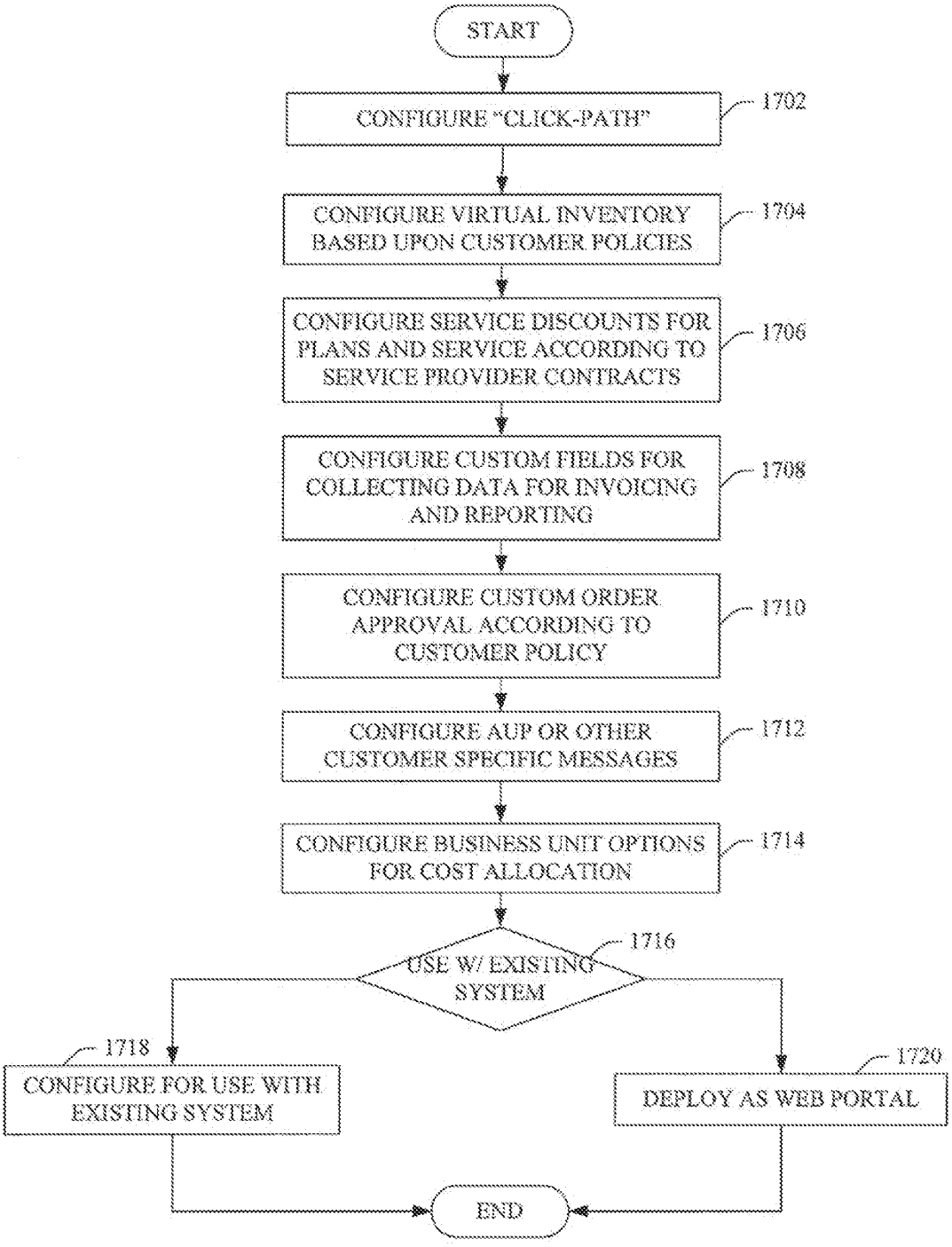

START
CONFIGURE "CLICK-PATH"
1702
CONFIGURE VIRTUAL INVENTORY BASED UPON CUSTOMER POLICIES
1704
CONFIGURE SERVICE DISCOUNTS FOR PLANS AND SERVICE ACCORDING TO SERVICE PROVIDER CONTRACTS
1706
CONFIGURE CUSTOM FIELDS FOR COLLECTING DATA FOR INVOICING AND REPORTING
1708
CONFIGURE CUSTOM ORDER APPROVAL ACCORDING 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 | 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 |
| Y | | 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<br>Mail Stop PCT, Attn: ISA/US, Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201 | Authorized officer:<br>Lee W. Young<br>PCT Helpdesk: 571-272-4300<br>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.*

WO 2004/077797 A2

(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.

# 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 S1 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 accesses 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 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 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.

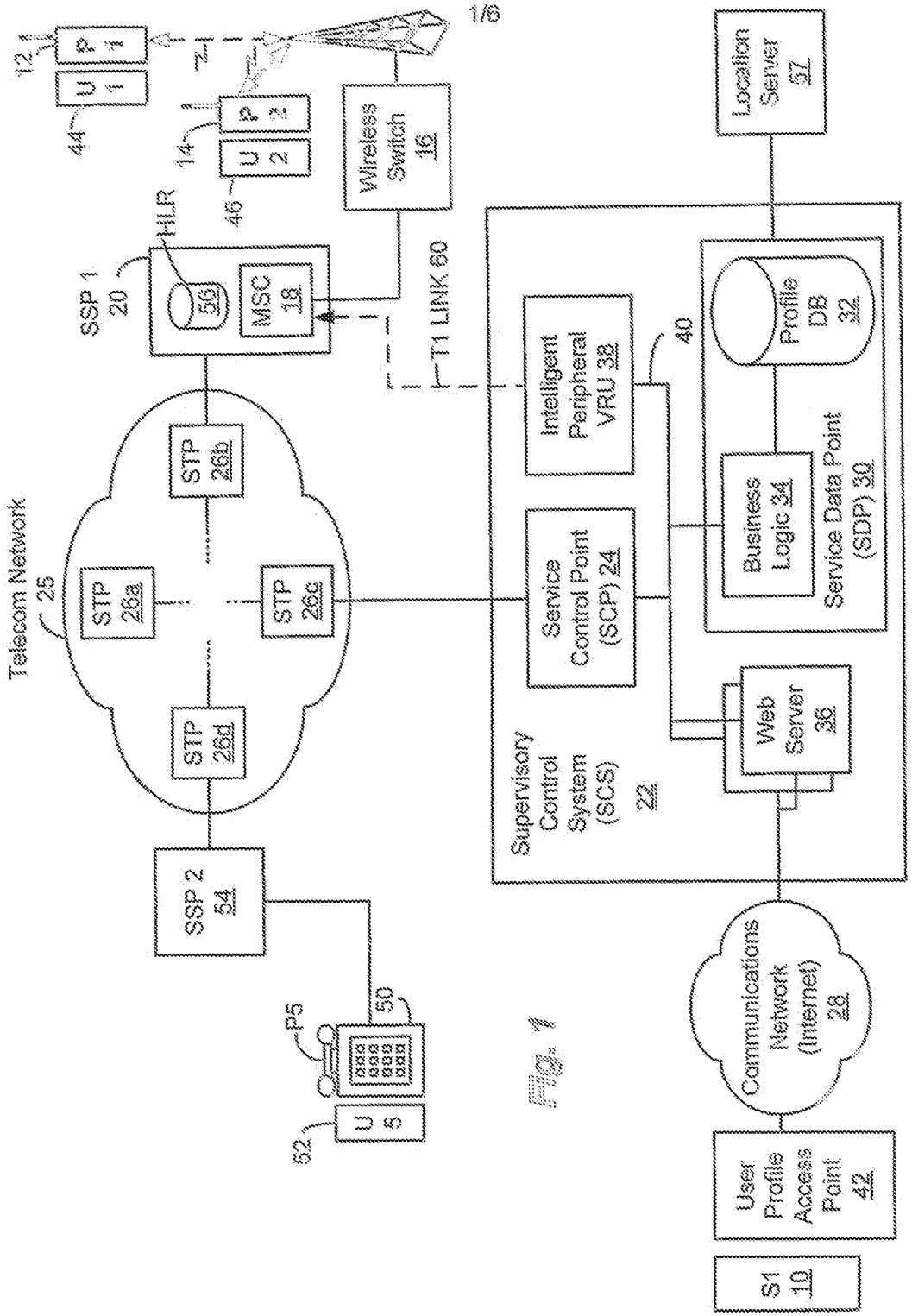

1/6
Location Server 57
Wireless Switch 16
T1 LINK 60
SSP 1 20
HLR 56
MSC 18
Telecom Network 25
STP 26a
STP 26b
STP 26c
STP 26d
SSP 2 54
Intelligent Peripheral VRU 32
Service Control Point (SCP) 24
Profile DB 32
Business Logic 34
Service Data Point (SDP) 30
Supervisory Control System (SCS) 22
Web Server 36
Communications Network (Internet) 28
User Profile Access Point 42
S1 10
U 1
U 2
U 5
P 1
P 2
P5
12
14
44
46
50
52
40

Fig. 1

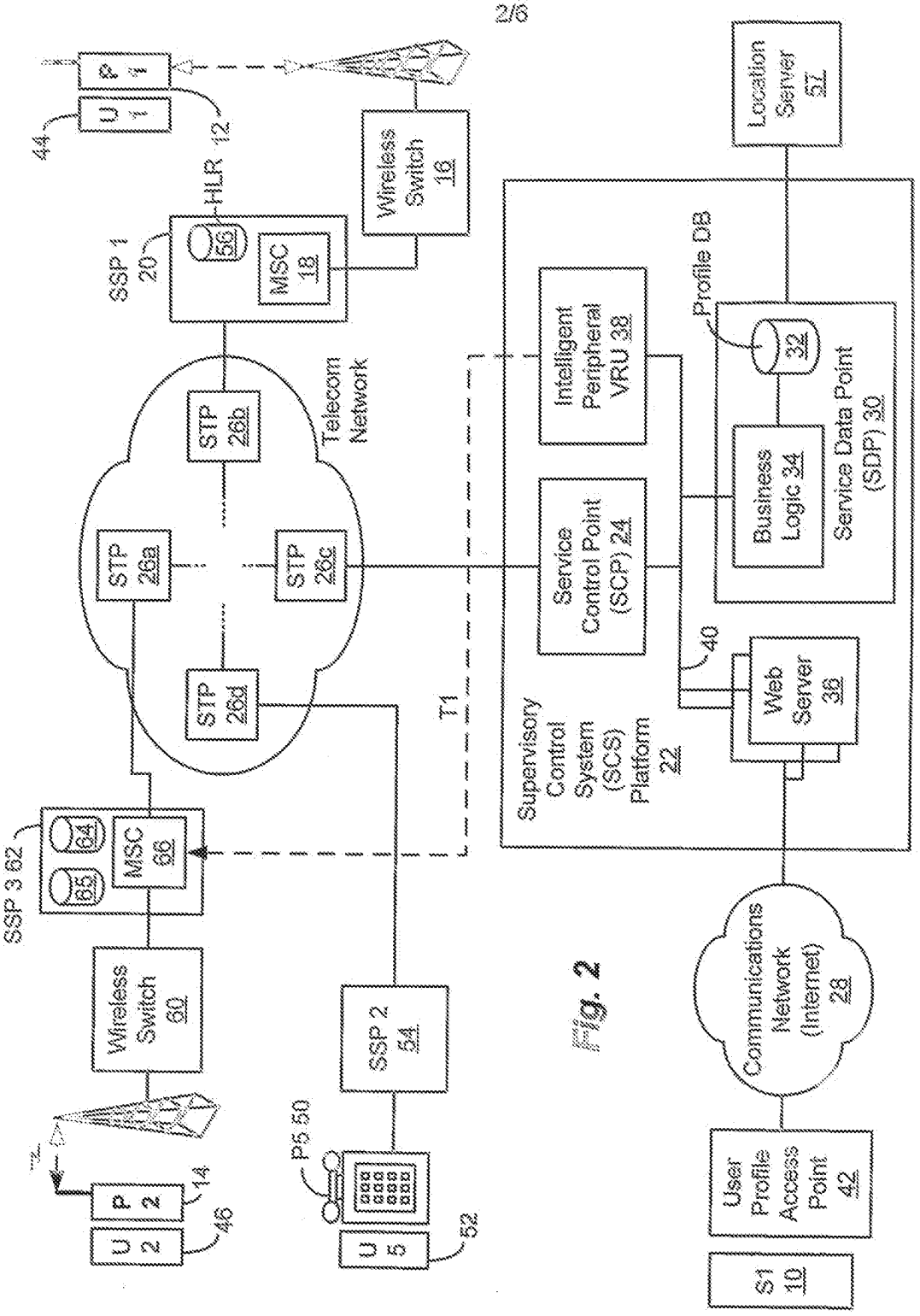

S1 10
User Profile Access Point 42
Communications Network (Internet) 28
Location Server 57
Profile DB
32
Business Logic 34
Service Data Point (SDP) 30
Intelligent Peripheral VRU 38
Service Control Point (SCP) 24
Supervisory Control System (SCS) Platform 22
Web Server 36
40
T1
Telecom Network
STP 26a
STP 26b
STP 26c
STP 26d
SSP 1 20
HLR 66
MSC 18
Wireless Switch 16
44
12
SSP 3 62
64
65
MSC 66
Wireless Switch 60
14
46
SSP 2 54
P5 50
52

*Fig. 2*

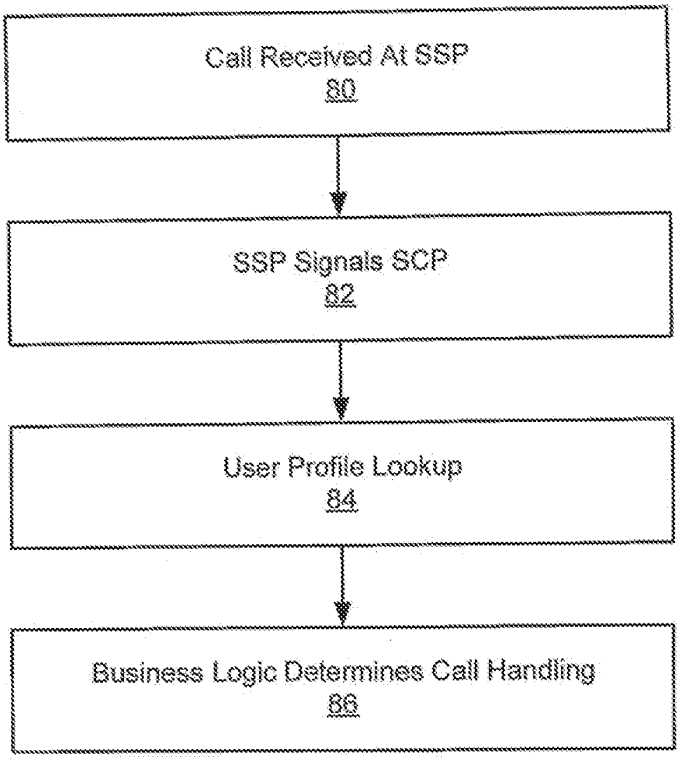

Call Received At SSP
80
SSP Signals SCP
82
User Profile Lookup
84
Business Logic Determines Call Handling
86

*Fig. 3*

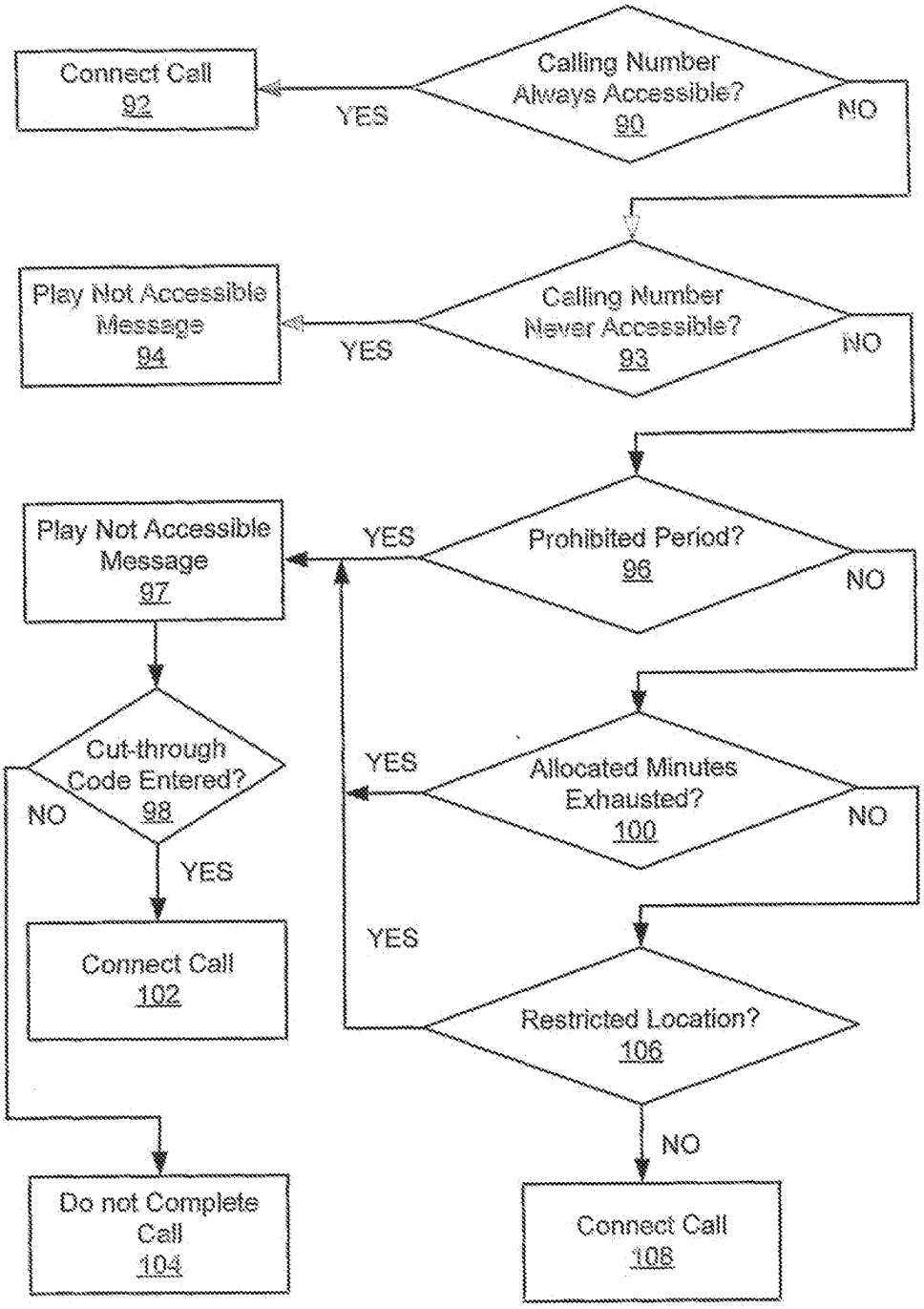

Calling Number Always Accessible? 90
YES
Connect Call 92
NO
Calling Number Never Accessible? 93
YES
Play Not Accessible Message 94
NO
Prohibited Period? 96
YES
Play Not Accessible Message 97
NO
Allocated Minutes Exhausted? 100
YES
NO
Restricted Location? 106
YES
NO
Cut-through Code Entered? 98
NO
YES
Connect Call 102
Do not Complete Call 104
Connect Call 108

*Fig. 4*

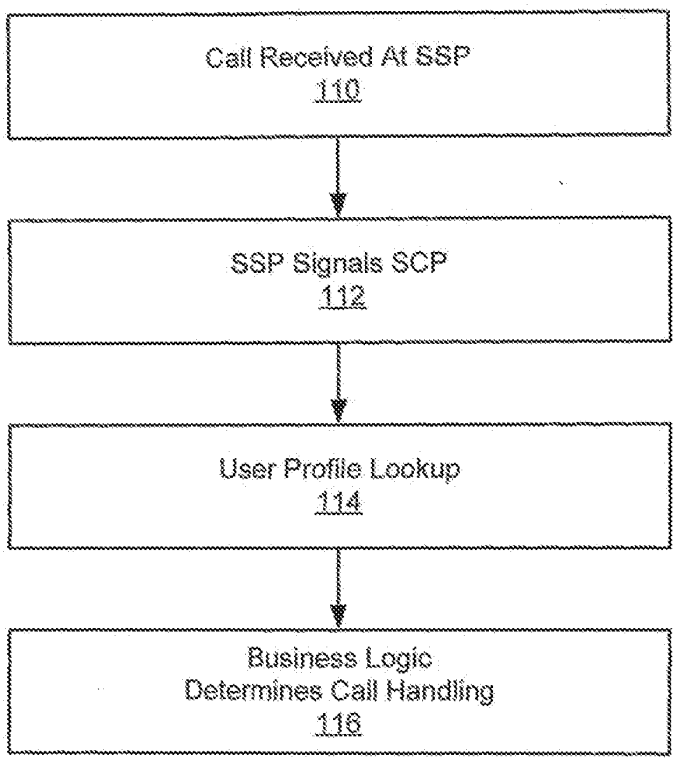

Call Received At SSP
110
SSP Signals SCP
112
User Profile Lookup
114
Business Logic
Determines Call Handling
116

*Fig. 5*

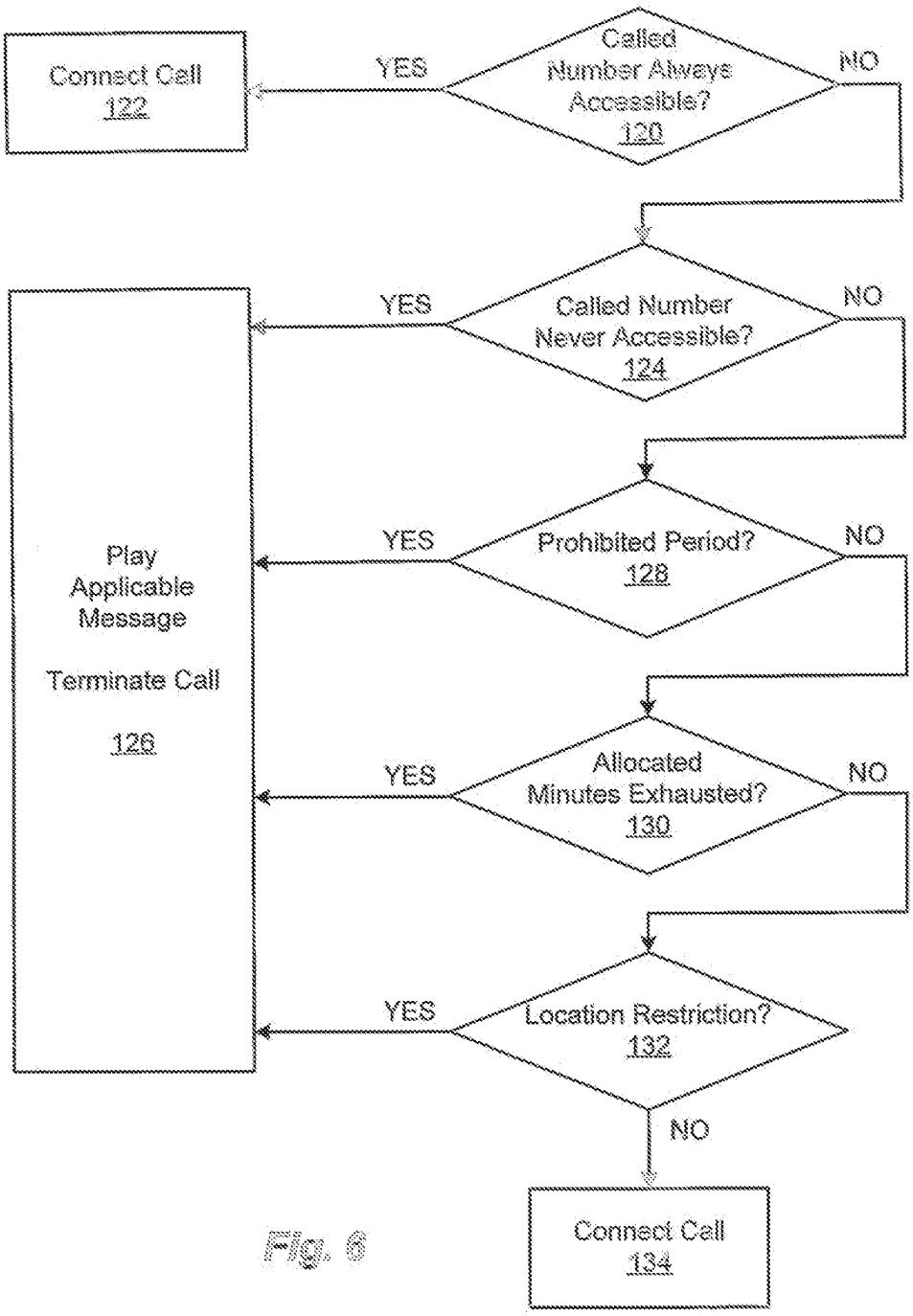

Called Number Always Accessible? 120
YES
NO
Connect Call 122
Called Number Never Accessible? 124
YES
NO
Prohibited Period? 128
YES
NO
Allocated Minutes Exhausted? 130
YES
NO
Location Restriction? 132
YES
NO
Play Applicable Message
Terminate Call
126
Connect Call 134

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).

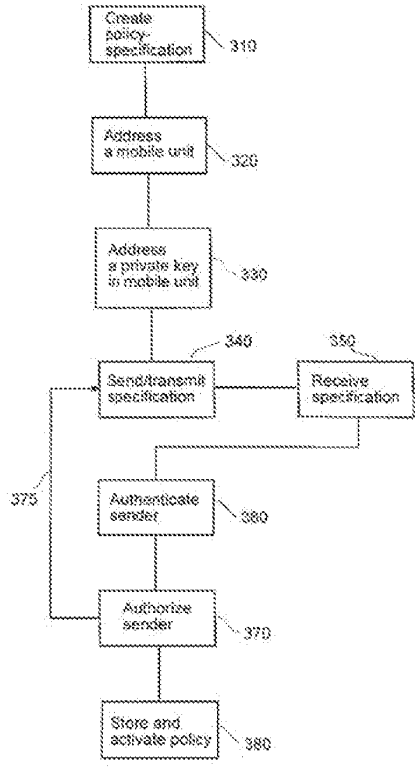
(74) Agent: **SVENSSON, Peder**; Telia Research AB, Vitsandsgatan 9, S-123 86 Farsta (SE).

(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.

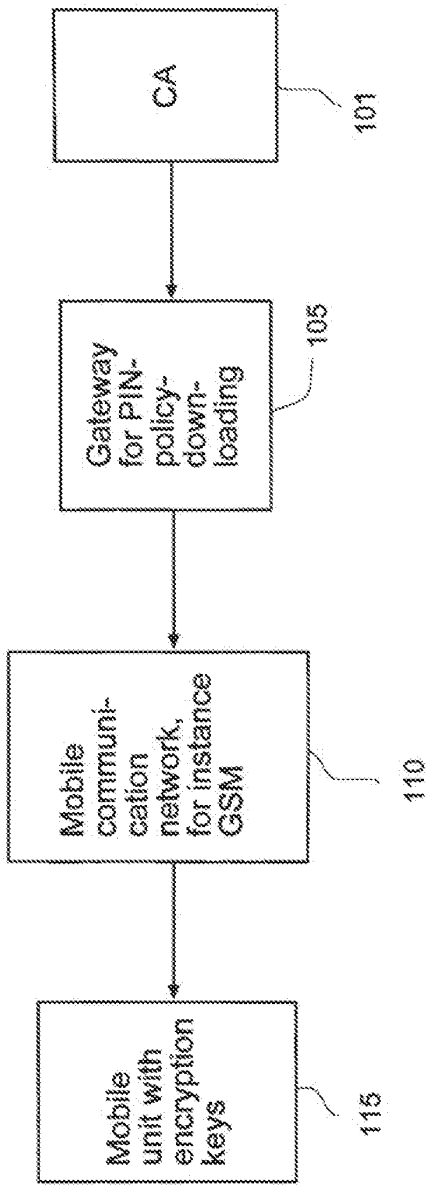

CA
101
Gateway for PIN-policy-down-loading
105
Mobile communi-cation network, for instance GSM
110
Mobile unit with encryption keys
115

Figure 1

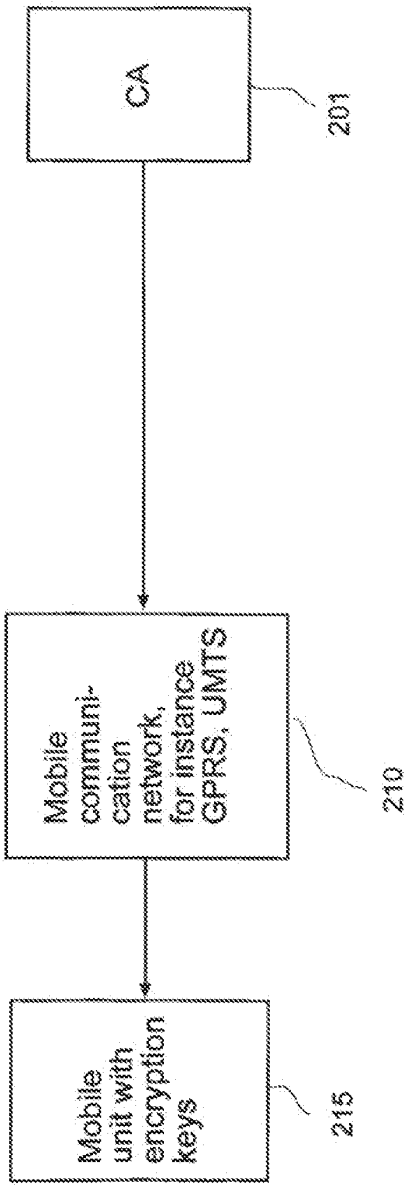

CA
201
Mobile communi-cation network, for instance GPRS, UMTS
210
Mobile unit with encryption keys
215

Figure 2

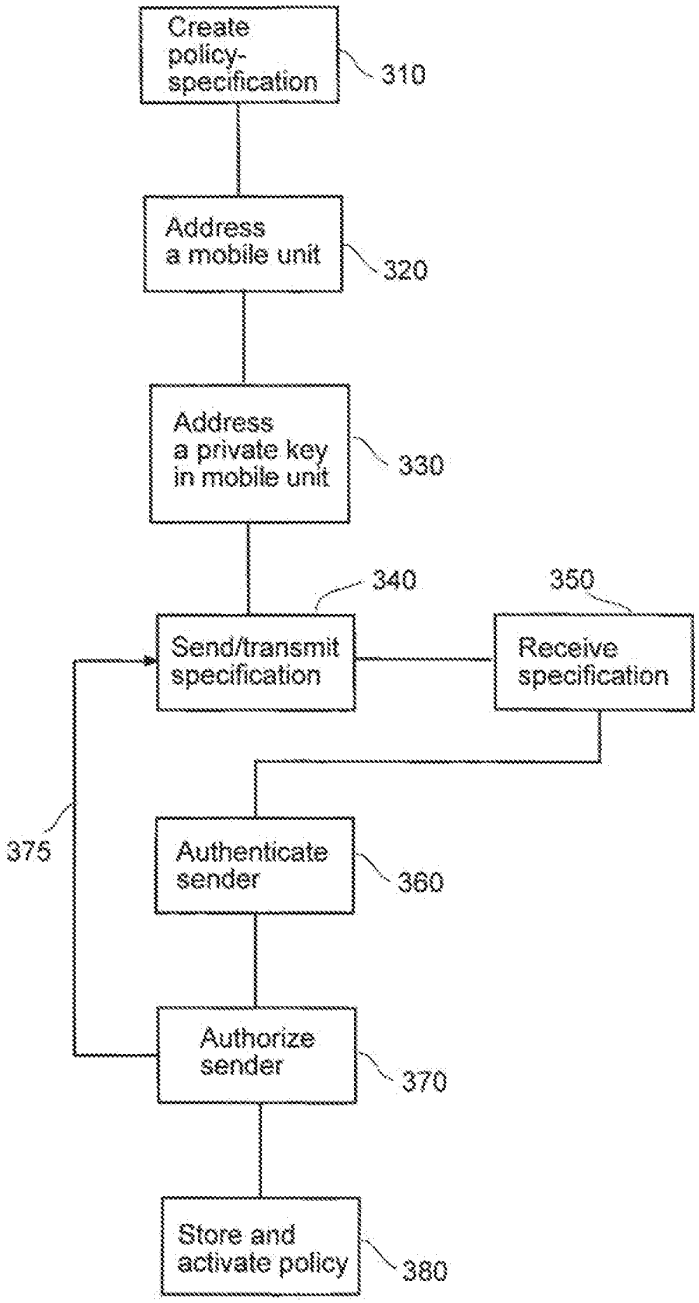

Create policy-specification
310
Address a mobile unit
320
Address a private key in mobile unit
330
340
350
Send/transmit specification
Receive specification
375
Authenticate sender
360
Authorize sender
370
Store and activate policy
380

Figure 3

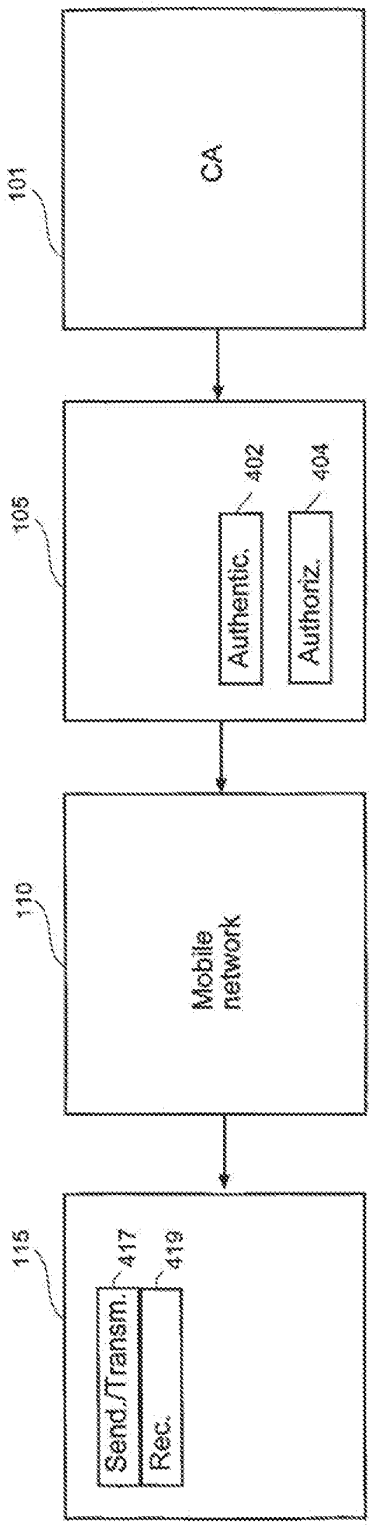



Figure 4A

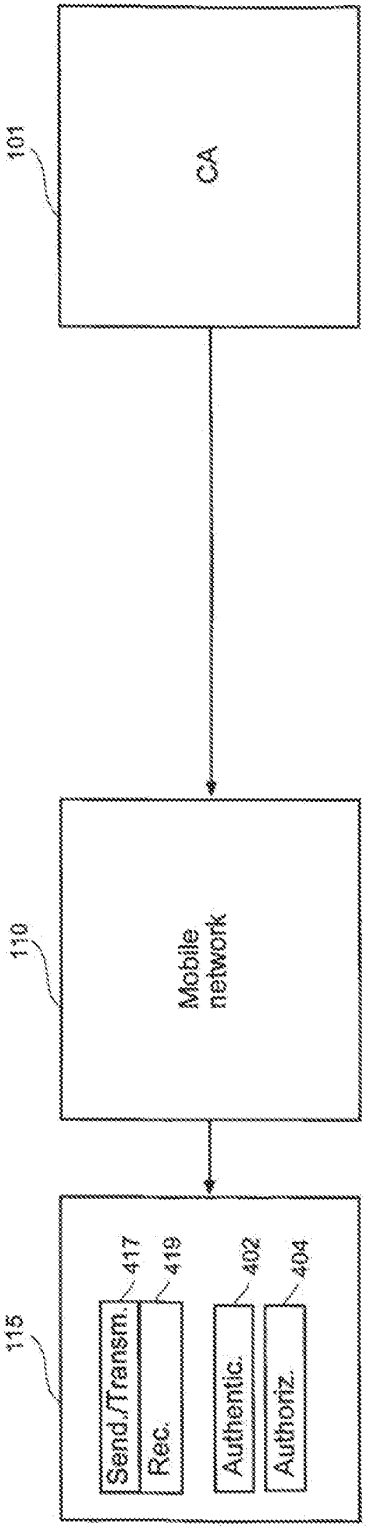



Figure 4B

# 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<br>--- | 1-14 |
| A | WO 0135685 A1 (MOBILIX A/S), 17 May 2001 (17.05.01), abstract, cited in the application<br>--- | 1-14 |
| A | US 5944824 A (HE, J.), 31 August 1999 (31.08.99), claim 1<br>--- | 1-14 |
| A | US 4924514 A (MATYAS, S.M. ET AL), 8 May 1990 (08.05.90), cited in the application<br>--- | 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
"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 |
|---|---|
| 7 April 2003 | 09-04-2003 |
| Name and mailing address of the ISA/<br>Swedish Patent Office<br>Box 5055, S-102 42 STOCKHOLM<br>Facsimile No. +46 8 666 02 86 | Authorized officer<br>Rune Bengtsson/mj<br>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<br><br>--<br>-------- | 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:** | 8297709 |
| **Application Number:** | 12694445 |
| **International Application Number:** | |
| **Confirmation Number:** | 6030 |
| **Title of Invention:** | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES |
| **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:** | RALEP025 |
| **Receipt Date:** | 27-AUG-2010 |
| **Filing Date:** | 27-JAN-2010 |
| **Time Stamp:** | 16:07:01 |
| **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 | RALEP025_IDS_Before_1st_OA.pdf | 56034<br>b36609e32bb1573319e137a68cec19f5bb392ab0 | no | 2 |

| | |
|---|---|
| **Warnings:** | |
| **Information:** | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | Information Disclosure Statement (IDS) Filed (SB/08) | RALEP025_IDS_SB08_2.pdf | 89834<br>eb59d83777ccbdce14424f67f00f8716819a5680 | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| This is not an USPTO supplied IDS fillable form | | | | | |
| 3 | Foreign Reference | RALE_Foreign_Ref_2A.pdf | 5821505<br>81bd528285eeb7055e34118b1c6f3ad0b406f580 | no | 34 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 4 | Foreign Reference | RALE_Foreign_Ref_2B.pdf | 4014433<br>6c150dbecf6e07e6e926c4953d9f7fa596419ee3 | no | 26 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 5 | Foreign Reference | RALE_Foreign_Ref_2C.pdf | 8969766<br>8a08a661fedb57f7c563ba498f498bb2309c2fc6 | no | 61 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 6 | Foreign Reference | RALE_Foreign_Ref_2D.pdf | 12405145<br>775980dffc4fd87b178f106d99003d7a52ddaca2 | no | 79 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 7 | Foreign Reference | RALE_Foreign_Ref_2E.pdf | 2436174<br>c0f643662921a19d681c882cd985d04b7837a8bd | no | 21 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 8 | NPL Documents | RALE_NPL_Ref_2F.pdf | 219474<br>ebce1f8721f1fe656f69a3905f36d944f0f575a4 | no | 6 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 9 | NPL Documents | RALE_NPL_Ref_2G.pdf | 682711<br>8ee373cfd5a9d752aae23b4ea2fc1e12b949497c | no | 77 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 10 | NPL Documents | RALE_NPL_Ref_2H.pdf | 137925<br>312ccdc04271430ed42b709573c0105d48599e5d | no | 8 |

| | | | | | |
|---|---|---|---|---|---|
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 11 | NPL Documents | RALE_NPL_Ref_2I.pdf | 1378815<br>1d1b86ccc61e4d602380d993e4561849720eab8b | no | 17 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 12 | NPL Documents | RALE_NPL_Ref_2J.pdf | 1319237<br>50d69a59a8af2531967879de03d70ef081c646f2 | no | 5 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 13 | NPL Documents | RALE_NPL_Ref_2K.pdf | 384366<br>ca4acdc0719ea1636b3d667e2aafd3397dfca7ef | no | 23 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 14 | NPL Documents | RALE_NPL_Ref_2L.pdf | 3636374<br>8440928107fdb5d75ce06783a2192520dc545702 | no | 15 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 15 | NPL Documents | RALE_NPL_Ref_2M.pdf | 887279<br>5a30977e77dc57a16d92c2240fea93e245299f94 | no | 111 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 16 | NPL Documents | RALE_NPL_Ref_2N.pdf | 2190991<br>8ba9616337a9da73d1158dfaec561ac7bc23b576 | no | 219 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 17 | NPL Documents | RALE_NPL_Ref_2O.pdf | 22848329<br>5dfb6b37b9bdba2974aea1f1643a2cc9b9129f17 | no | 262 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 18 | NPL Documents | RALE_NPL_Ref_2P.pdf | 496028<br>a267ff12b9b336818993ff8b85da8e35a5708cc5 | no | 35 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 19 | NPL Documents | RALE_NPL_Ref_2Q.pdf | 1970806<br>2398c7ca475eec3e037b4ad60021644397a754ed | no | 10 |

| | | | | | |
|---|---|---|---|---|---|
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 20 | NPL Documents | RALE_NPL_Ref_2R.pdf | 347340<br>e87bfc75fa6949a4c1ea09d431b076cdc1b55249 | no | 11 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| | | | **Total Files Size (in bytes):** | 70292566 | |

**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.: | 12/694,445 | Art Unit: | 2614 |
| Filed: | January 27, 2010 | Docket No.: | RALEP025 |
| Title: | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | | |

## 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. RALEP025).

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|---|---|---|---|
| 12/694,445 | 01/27/2010 | Gregory G. Raleigh | RALEP025 |

**CONFIRMATION NO. 6030**

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

**PUBLICATION NOTICE**

*OC000000042918305*

**Title:**SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

**Publication No.**US-2010-0199325-A1
**Publication Date:**08/05/2010

## NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

---

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

| APPLICATION NUMBER | FILING or 371(c) DATE | GRP ART UNIT | FIL FEE REC'D | ATTY.DOCKET.NO | TOT CLAIMS | IND CLAIMS |
|---|---|---|---|---|---|---|
| 12/694,445 | 01/27/2010 | 2614 | 1480 | RALEP025 | 25 | 3 |

**CONFIRMATION NO. 6030**

**UPDATED FILING RECEIPT**

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

*OC000000041274174*

Date Mailed: 04/26/2010

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

**Applicant(s)**

Gregory G. Raleigh, Woodside, CA;

**Assignment For Published Patent Application**

HEADWATER PARTNERS I LLC, Woodside, CA

**Power of Attorney:** The patent practitioners associated with Customer Number 21912

**Domestic Priority data as claimed by applicant**

This application is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009

**Foreign Applications**

**If Required, Foreign Filing License Granted:** 02/17/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/694,445**

**Projected Publication Date:** 08/05/2010

**Non-Publication Request:** No

**Early Publication Request:** No

**Title**

SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

**Preliminary Class**

379

## PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

## LICENSE FOR FOREIGN FILING UNDER

## Title 35, United States Code, Section 184

## Title 37, Code of Federal Regulations, 5.11 & 5.15

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

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

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

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

# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Inventor: | Gregory G. Raleigh | Examiner: | Not Assigned |
| Application No.: | 12/694,445 | Art Unit: | 2614 |
| Filed: | January 27, 2010 | Docket No.: | RALEP025 |
| Title: | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | | |

## RESPONSE TO NOTICE TO FILE MISSING PARTS

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

Sir:

This is a Response to Notice to File Missing Parts mailed **February 22, 2010.**

Application Elements:

☒ Declaration

☒ Newly executed (original or copy)

☐ Copy from a prior application (37 CFR 1.63(d) for a continuation or divisional). The entire disclosure of the prior application from which a copy of the declaration is herein supplied is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

☐ Deletion of inventors Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

Accompanying Application Parts:

☐ Information Disclosure Statement with Form PTO/SB/08 ☐ Copies of IDS Citations

☐ Preliminary Amendment (*New claims numbered after highest original claim in prior application.*)

☐ Return Receipt Postcard

☐ Copy of Notice to File Missing Parts of NonProvisional Application

☐ Other:

Amendments

☐ Cancel in this application original claims _____ of the prior application before calculating the filing fee. (*At least one original independent claim must be retained.*)

Fee Calculation (37 CFR § 1.16)

| | | | | | Small Entity | | | Large Entity | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Rate | Fee | | Rate | Fee |
| Filing Fees | | | | | x $165 = $ | | OR | x $330 = $ | 330 |
| Search Fees | | | | | x $270 = $ | | OR | x $540 = $ | 540 |
| Examination Fees | | | | | x $110 = $ | | OR | x $220 = $ | 220 |
| CLAIMS | Filed. | | Extra | | | | | | |
| Total | 25 | Less 20 | 5 | | x $26 = $ | | OR | x $52 = $ | 260 |
| Independent | 3 | Less 3 | -0- | | x $110 = $ | | OR | x $220 = $ | |
| Multiple Dependent Claims | | | -0- | | x $195 = $ | | OR | x $390 = $ | |
| Declaration and Surcharge Fee | | | | | X $65 = $ | | OR | X $130 = $ | 130 |
| | | | | | TOTAL FILING FEE $ | | | TOTAL FILING FEE $ | **1480.00** |

☐ Applicants petition for an extension of time to respond under 37 CFR § 1.136(a) as follows:

| | | SMALL ENTITY | | | LARGE ENTITY | |
|---|---|---|---|---|---|---|
| | | Rate | Add'l Fee | | Rate | Add'l Fee |
| ☐ Extension for Response within FIRST month | | x $65 = $ | | OR | x $130 = $ | |
| ☐ Extension for Response within SECOND month | | x $245 = $ | | OR | x $490 = $ | |
| ☐ Extension for Response within THIRD month | | x $555 = $ | | OR | x $1110 = $ | |
| ☐ Extension for Response within FOURTH month | | x $865 = $ | | OR | x $1730= $ | |
| ☐ Extension for Response within FIFTH month | | x $1175 = $ | | OR | x $2350 = $ | |

☐ Check No. _____for $_____ is enclosed.

General Authorizations

☒ Applicants hereby make and generally authorize any Petitions for Extensions of Time as needed for this or any subsequent filings. The Commissioner is also authorized to charge any extension fees under 37 CFR §1.17 as needed to Deposit Account No. 50-0685 (Order No. RALEP025).

☒ The Commissioner is given general authorization to charge any fees or to credit any overpayment during the pendency of this application to Deposit Account No. 50-0685 (Order No. RALEP025).

☒ Please send correspondence to the following address:

**Customer No. 21912**
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd.
Suite 200
Cupertino, CA 95014

Date: April 15, 2010

/Michael J. Schallop/
Michael J. Schallop
Registration No. 44,319

# DECLARATION AND POWER OF ATTORNEY FOR ORIGINAL U.S. PATENT APPLICATION

Attorney's Docket No. RALEP025

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES**, the specification of which,

(check one)

1. ☐ is attached hereto.

2. ☒ was filed on January 27, 2010 as U.S. Application No. 12/694,445 and was amended on _____.

3. ☐ was filed on _____ as International PCT Application No. _____ and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

*For Assigned Inventions*: I understand that the purpose of making this appointment is to permit prosecution of patent applications for the above-identified invention for the benefit of my assignee, and that this appointment does not create an attorney-client relationship between me and these appointees.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under Title 35, United States code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

**Prior Foreign Application(s)** Priority Benefits Claimed?

| (Appl. No.) | (Country) | (Filing Date) | ☐Yes ☐No |
|---|---|---|---|
| | | | |

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

**Prior Provisional Application(s)**

| (Application No.) | (Filing Date) |
|---|---|
| 61/206,354 | 1/28/2009 |
| 61/206,944 | 2/4/2009 |

| | |
|---|---|
| 61/207,393 | 2/10/2009 |
| (Application No.) | (Filing Date) |
| 61/207,739 | 2/13/2009 |
| (Application No.) | (Filing Date) |
| 61/252,151 | 10/15/2009 |
| (Application No.) | (Filing Date) |

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

**Prior U.S. Application(s)**

| | | |
|---|---|---|
| 12/380,780 | 03/02/2009 | PENDING |
| (Application No.) | (Filing Date) | (Status - patented, pending, abandoned) |

And I hereby appoint the attorneys and/or agents associated with Customer No. **21912** as my principal attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

**Please Direct all Correspondence To:** **Customer No. 21912**
VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014

**Direct Telephone Calls To:** **Michael J. Schallop at telephone number (408) 207-4762**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

| | | | | | |
|---|---|---|---|---|---|
| Full name of sole or first inventor | Gregory G. Raleigh | | | | |
| Signature of sole or first inventor | | | | Date: | 4/8, 2010 |
| Residence: City | Woodside | State: | CA | Citizenship: | US |
| Mailing Address | 2995 Woodside Road, Suite 400, Woodside, CA 94062 | | | | |

# Electronic Patent Application Fee Transmittal

| | |
|---|---|
| **Application Number:** | 12694445 |
| **Filing Date:** | 27-Jan-2010 |
| **Title of Invention:** | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES |
| **First Named Inventor/Applicant Name:** | Gregory G. Raleigh |
| **Filer:** | Michael J. Schallop/Veronica Pula |
| **Attorney Docket Number:** | RALEP025 |

Filed as Large Entity

## Utility under 35 USC 111(a) Filing Fees

| Description | Fee Code | Quantity | Amount | Sub-Total in USD($) |
|---|---|---|---|---|
| **Basic Filing:** | | | | |
| Utility application filing | 1011 | 1 | 330 | 330 |
| Utility Search Fee | 1111 | 1 | 540 | 540 |
| Utility Examination Fee | 1311 | 1 | 220 | 220 |
| **Pages:** | | | | |
| **Claims:** | | | | |
| Claims in excess of 20 | 1202 | 5 | 52 | 260 |
| **Miscellaneous-Filing:** | | | | |
| Late filing fee for oath or declaration | 1051 | 1 | 130 | 130 |

| Description | Fee Code | Quantity | Amount | Sub-Total in USD($) |
|---|---|---|---|---|
| **Petition:** | | | | |
| **Patent-Appeals-and-Interference:** | | | | |
| **Post-Allowance-and-Post-Issuance:** | | | | |
| **Extension-of-Time:** | | | | |
| **Miscellaneous:** | | | | |
| | | **Total in USD ($)** | | **1480** |

| Electronic Acknowledgement Receipt | |
|---|---|
| **EFS ID:** | 7429493 |
| **Application Number:** | 12694445 |
| **International Application Number:** | |
| **Confirmation Number:** | 6030 |
| **Title of Invention:** | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES |
| **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:** | RALEP025 |
| **Receipt Date:** | 16-APR-2010 |
| **Filing Date:** | 27-JAN-2010 |
| **Time Stamp:** | 17:18:17 |
| **Application Type:** | Utility under 35 USC 111(a) |

## Payment information:

| | |
|---|---|
| Submitted with Payment | yes |
| Payment Type | Deposit Account |
| Payment was successfully received in RAM | $1480 |
| RAM confirmation Number | 3797 |
| Deposit Account | 500685 |
| Authorized User | |
| The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:<br>Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges) | |

## File Listing:

| Document Number | Document Description | File Name | File Size(Bytes)/ Message Digest | Multi Part /.zip | Pages (if appl.) |
|---|---|---|---|---|---|
| 1 | Miscellaneous Incoming Letter | RALEP025_Response_to_Missing_Parts.pdf | 83692<br>06436f7976bf0198e371c0d3eee184005629f84f | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 2 | Oath or Declaration filed | RALEP025_Declaration_POA.pdf | 465365<br>cf1f110722069a8404077c6da27e5ff6d2339001 | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| 3 | Fee Worksheet (PTO-875) | fee-info.pdf | 38366<br>473cbef95cb0f57e364c1454bd710414180dd085 | no | 2 |
| **Warnings:** | | | | | |
| **Information:** | | | | | |
| | | **Total Files Size (in bytes):** | 587423 | | |

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

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

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|---|---|---|---|
| 12/694,445 | 01/27/2010 | Gregory G. Raleigh | RALEP025 |

**CONFIRMATION NO. 6030**

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

**FORMALITIES LETTER**

*OC000000040123118*

Date Mailed: 02/22/2010

# NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

**FILED UNDER 37 CFR 1.53(b)**

***Filing Date Granted***

**Items Required To Avoid Abandonment:**

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  *Applicant must submit $**330** to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*
- The oath or declaration is missing.
  *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
  *Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.*

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of $**260** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**130** for a non-small entity, must be submitted with the missing items identified in this notice.

**SUMMARY OF FEES DUE:**

Total additional fee(s) required for this application is $**1480** for a non-small entity
- $**330** Statutory basic filing fee.
- $**130** Surcharge.
- The application search fee has not been paid. Applicant must submit $**540** to complete the search fee.

- The application examination fee has not been paid. Applicant must submit $**220** to complete the examination fee for a non-small entity.
- Total additional claim fee(s) for this application is $**260**
  - $**260** for **5** total claims over 20.

Replies should be mailed to:

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

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/sduong/

---

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

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

| APPLICATION NUMBER | FILING or 371(c) DATE | GRP ART UNIT | FIL FEE REC'D | ATTY.DOCKET.NO | TOT CLAIMS | IND CLAIMS |
|---|---|---|---|---|---|---|
| 12/694,445 | 01/27/2010 | 2614 | 0.00 | RALEP025 | 25 | 3 |

**CONFIRMATION NO. 6030**

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

**FILING RECEIPT**

*OC000000040123117*

Date Mailed: 02/22/2010

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

**Applicant(s)**

Gregory G. Raleigh, Woodside, CA;

**Assignment For Published Patent Application**

HEADWATER PARTNERS I LLC, Woodside, CA

**Power of Attorney:** None

**Domestic Priority data as claimed by applicant**

This application is a CIP of 12/380,780 03/02/2009
and claims benefit of 61/206,354 01/28/2009
and claims benefit of 61/206,944 02/04/2009
and claims benefit of 61/207,393 02/10/2009
and claims benefit of 61/207,739 02/13/2009
and claims benefit of 61/252,151 10/15/2009

**Foreign Applications**

**If Required, Foreign Filing License Granted:** 02/17/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/694,445**

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

**Non-Publication Request:** No

**Early Publication Request:** No

**Title**

SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

**Preliminary Class**

379

## PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

## LICENSE FOR FOREIGN FILING UNDER

## Title 35, United States Code, Section 184

## Title 37, Code of Federal Regulations, 5.11 & 5.15

**GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

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

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

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

Attorney Docket No. RALEP025

# APPLICATION FOR UNITED STATES PATENT

## SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

By Inventor(s):

Gregory G. Raleigh
Woodside, CA
A Citizen of the United States

Assignee: Headwater Partners I LLC, a Delaware limited liability company

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014
Telephone (408) 973-2585

# SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

## CROSS REFERENCE TO OTHER APPLICATIONS

**[0001]** This application claims priority to U.S. Provisional Patent Application No. 61/206,354 (Attorney Docket No. RALEP001+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed January 28, 2009, U.S. Provisional Patent Application No. 61/206,944 (Attorney Docket No. RALEP002+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 4, 2009, U.S. Provisional Application No. 61/207,393 (Attorney Docket No. RALEP003+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009, U.S. Provisional Patent Application No. 61/207,739 (Attorney Docket No. RALEP004+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on February 13, 2009, and U.S. Provisional Patent Application No. 61/252,151 (Attorney Docket No. RALEP025+) entitled SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES, filed on October 15, 2009, which are incorporated herein by reference for all purposes.

**[0002]** This application is a continuation in part of co-pending U.S. Patent Application No. 12/380,780 (Attorney Docket No. RALEP007), entitled AUTOMATED DEVICE PROVISIONING AND ACTIVATION, filed on March 2, 2009, which is incorporated herein by reference for all purposes, and which claims priority to U.S. Provisional Patent Application No. 61/206,354 (Attorney Docket No. RALEP001+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed January 28, 2009, U.S. Provisional Patent Application No. 61/206,944 (Attorney Docket No. RALEP002+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 4, 2009, U.S. Provisional Application No. 61/207,393 (Attorney Docket No. RALEP003+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009, and U.S. Provisional Patent Application No. 61/207,739 (Attorney Docket No. RALEP004+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on February 13, 2009, which are incorporated herein by reference for all purposes.

## BACKGROUND OF THE INVENTION

**[0003]** With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), DOCSIS, DSL, and Wi-Fi (Wireless Fidelity) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum and cell splitting being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

**[0004]** Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0005]** Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

**[0006]** **Figure 1** illustrates a secure execution environment for device assisted services in accordance with some embodiments.

**[0007]** **Figure 2** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0008]** **Figure 3** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0009]** **Figure 4** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0010]** **Figure 5** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0011]** **Figure 6** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0012]** **Figure 7** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0013]** **Figure 8** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0014]** **Figure 9** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0015]** **Figure 10** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

**[0016]** **Figure 11** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

## DETAILED DESCRIPTION

**[0017]** The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term 'processor' refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

**[0018]** A detailed description of one or more embodiments of the invention is provided below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

**[0019]** In some embodiments, security techniques for device assisted services are provided. In some embodiments, secure service measurement and/or control execution partition techniques for device assisted services are provided. In some embodiments, a secure execution environment for device assisted services is provided. In some embodiments, a secure stack for device assisted services is provided. In some embodiments, a secure memory for device assisted services is provided. In some embodiments, a secure modem for device assisted services is

provided (e.g., providing a secure communication link between the modem/modem driver and a service processor and/or agent on the device, such as a communications device or an intermediate networking device). In some embodiments, one or more secure monitoring points for device assisted services are provided. In some embodiments, one or more secure monitoring points with verification for device assisted services are provided (e.g., a secured monitoring point can be provided in a modem, which communicates securely to a secured execution environment in a CPU/processor, which can then verify such service usage measures). In some embodiments, a secure bus for device assisted services is provided. In some embodiments, a secure execution environment in the CPU/processor for device assisted services is provided. In some embodiments, secure access to a secure execution environment(s) for device assisted services is provided (e.g., securing communication from a bottom of the stack, such as modem drivers, which require credentials to access the bus as controlled by a service processor or secure agent on the device, and in which the traffic on the bus is encrypted). In some embodiments, various secure execution environments for device assisted services are provided using various hardware partition techniques (e.g., secure memory, secure modems, secure memory partition(s) in the CPU/processor), as described herein.

**[0020]** In some embodiments, device assisted services (DAS) provide for one or more of device based service usage measurements, service usage policy implementation, service usage accounting, service usage control, and any of the other functions described in various embodiments that assist, replace, and/or augment network based functions. For example, various DAS embodiments perform one or more of the following: facilitate and control activation to one or more access service networks; measure access and/or service usage on one or more access networks; control access and/or service usage on one or more access networks; account for different types of service usage on one or more access networks; implement quality of service (QOS) controls, collect and report QOS traffic demand, aggregate multiple device QOS demand reports to asses a measure of overall network QOS demand, and/or facilitate QOS resource allocation; and/or facilitate roaming between access networks. There are many more functions and embodiments for DAS as described with respect to various embodiments.

**[0021]** In some embodiments, various program/functional elements that perform the functions to implement various DAS embodiments are referred to herein as DAS agents or

device assisted service agents, or in some embodiments, more specific terms are used to be more descriptive in specific examples. In some embodiments, device assisted service agent functions include service measurements and/or service measure recording and/or service measure reporting (e.g., to the service controller, the device, the user, or other device agents) and/or service measure synchronization (e.g., between device and network). In some embodiments, device assisted service agent functions include service usage controls and/or service usage control policy settings. In some embodiments, service usage controls include one or more of network authorization, network authentication, network admission, access control, service usage activity classification, allowing or disallowing one or more service usage activity and traffic shaping for one or more service usage activity.

**[0022]** In some embodiments, device assisted service agent functions include one or more of the following: reporting service usage to QOS control elements in the network, receiving QOS assignment from the network, reporting QOS assignments to the network, and/or communicating with QOS service reservation elements in the network. In some embodiments, device assisted service agent functions include one or more of implementing QOS service controls on the device based on one or more of the following criteria: fair queuing of service usage activities, differentiated QOS based on an assigned QOS hierarchy of service usage activities, service usage activity QOS assignments from the network for one or more service usage activities, service usage activity policy directives from the network for one or more service usage activities.

**[0023]** In some embodiments, a service control link is used for communication between the device assisted service agents and the service controller. In some embodiments, the service control link is a secure link (e.g., an encrypted communication link).

**[0024]** In some embodiments, the device assisted service agent functions include device assisted service system communication, measuring and/or recording and/or reporting and/or synchronizing service measures, observing communicating information for service control integrity, communicating information for service control policy instructions and/or settings, or updating device assisted software and/or agent settings.

**[0025]** In some embodiments, device assisted service on the device includes the following: service measurements, service controls, user interface and usage reporting, user policy options, accept policy instructions, protected execution partition provided to prevent hacking, malware, errors, and other security techniques. In some embodiments, device assisted service on the server includes one or more of the following: set policy, set configurations, install/update agents, check usage versus policy, check proper operation of agents, synchronize usage from network to device, and other verification techniques. For example, when errors in policy enforcement are detected, servers can perform actions to either further observe, quarantine, or suspend the device.

**[0026]** In some embodiments, a control server/control service network element receives service measures from the device. In some embodiments, the control server/control service network element receives service measures from the network. In some embodiments, the control server/control service network element sets policies and manages service across multiple networks (e.g., while one modem is shown in various figures, multiple modems can be employed for multiple networks with consistent service usage measures, service controls, QOS controls, UI (User Interface), user preferences, user usage reporting, and/or other settings/controls across different networks).

**[0027]** In some embodiments, traffic type refers to one or more of the following: best effort network traffic, real-time traffic (e.g., live voice such as VOIP, live video, etc.), streaming traffic, multi-cast traffic, uni-cast traffic, point to point traffic, file types, traffic associated with an application, real time traffic, traffic with an assigned priority, traffic without an assigned priority, and traffic for a certain network.

**[0028]** In some embodiments, service usage activity refers to a usage of service by a device. In some embodiments, service usage activity can be one or more of connection to an access network, connection to certain destinations, URLs or addresses on a network, connection to the network by one or more applications, transmission of certain types of traffic, a type of transaction based service, a type of advertising based services, or a combination of one or more of the following: an application type, a network destination/address/URL, a traffic type, and a transaction type.

**[0029]** In some embodiments, protection of the device assisted service agents/functional elements to protect the functions that perform the device assisted functions is provided with a protected execution partition on the CPU (Central Processor Unit), APU (Auxiliary Processor Unit), or another hardware based processor. For example, such hardware protected execution capabilities in the CPU, APU, or other processor can be combined in some embodiments with either OS software functions or other native mode software functions to create secure program execution partitions as described herein. In some embodiments, the term host is used to refer to the hardware and firmware and/or software system that executes the device applications and networking stack. In some embodiments, some of the device assisted service agents/functions are implemented in a modem execution partition environment.

**[0030]** **Figure 1** illustrates a secure execution environment 100 (e.g., for a communications device) for device assisted services in accordance with some embodiments. As shown in Figure 1, the device execution environments include program/functional elements for a communications (e.g., a communications device can be an intermediate networking device, such as 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems, DSL modems, remote access/backup routers, and other intermediate network devices, or a mobile communications device, such as a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, a tablet, a home networking system, and/or any other mobile communications device) device that utilizes the modem subsystems #1 (125) through #N (127) to connect to one or more of the access networks #1 (136) through #N (138). In some embodiments, a communications device includes multiple program execution partitions. As shown in Figure 1, four execution partitions are provided: an application execution partition 102 in which, for example, application programs execute, a kernel execution partition 112 in which, for example, the lower level drivers and basic low level OS programs execute, a protected device assisted service (DAS) execution partition 114 (also referred to as protected DAS partition) in which, in some embodiments, some or all of the device assisted service agents and/or functions execute, and a modem execution partition 124 in which, for example, the modem program elements execute and, in some embodiments, some or all of the device assisted service agents and/or functions execute. In some embodiments, each of these execution partitions are optimized for different software functions, each providing programs with the basic physical memory, data memory, CPU or APU or modem processor execution

resources, high level and/or low level OS, memory management, file storage, I/O device resources (e.g., user interface (UI), peripherals, etc.), network communications stack, other device resources, and/or other resources that are required or used for operation of the programs. The collection of these hardware and software resources for the CPU or APU is sometimes referred to herein with the term host.

**[0031]** As shown, Figure 1 illustrates an application execution partition 102 and a kernel execution partition 112, which are shown as separate partitions within the device execution environments. For example, this separation is based on the manner in which "kernel programs" (e.g., drivers and network stack, etc.) are commonly supported as compared to "application programs" (e.g., browsers, word processors, user interfaces, etc.) within the context of several different popular operating systems (OS) (e.g., Windows, UNIX, Linux, MAC OS, certain mobile device OSs, certain embedded device OSs, etc.). In some embodiments, this functional separation is not required, and, in some embodiments, other functional separations are supported.

**[0032]** As shown in Figure 1, protected device assisted service agents, such as the protected DAS partition device assisted service agents 110, execute in the protected DAS partition 114 while unprotected device assisted service agents and/or OS networking stack elements and applications (e.g., applications 106A through 106C) execute outside of the secure device assisted service execution partition 114, such as the application partition device assisted service agents 104 and the OS networking stack and/or kernel partition device assisted service agents 108. For example, the protected DAS partition 114 can make it more difficult for a hacker, malware or system errors to compromise, attack or modify the device assisted service measurements, service policy implementation or service usage control operations on the device (e.g., communications device). In some embodiments, the protected DAS partition 114 need not support open access to all programs and OS elements so that it can be easier to protect. Also, as shown, a bus driver 116 in the application execution partition 102 provides for communication with a modem bus 120, which is in communication with a bus driver 121 in the modem execution partition 124. The protected DAS partition also includes a host service control link 118, which facilitates communication with a host secure channel 150 as shown.

**[0033]** In some embodiments, the protected DAS partition 114 is a protected execution partition on the main device that is supported by certain configurations in the host (e.g., a secure virtual execution environment or a separate hardware security function). For example, this protected execution partition can be used to provide added service measurement integrity and/or service control integrity for a device assisted service enabled device. In some embodiments, as described herein, the operating system (OS) also performs a role in establishing the protected execution partition for secure operation of device assisted services, and, in some embodiments, this role is performed by native software or firmware operating on secure hardware elements.

**[0034]** In some embodiments, the DAS agents responsible for maintaining service control integrity execute in the protected DAS partition 114. For example, the protected DAS partition device assisted service agents 110 can include one or more of the following: one or more service usage measurement functions; some or all of the device networking stack functions that are monitored and/or controlled by the device assisted services system; device drivers that interface to an OS networking stack to observe or manipulate stack traffic; access control integrity functions; service policy control functions; service UI functions; application identification functions, and/or functions to classify service usage activities by combinations of application, address/URL and/or traffic type; modem bus driver functions; and/or modem data encryption functions to prevent other unauthorized programs from bypassing the device assisted service measurements and/or controls by directly accessing the modem around the stack. In some embodiments, the system designer or a given set of design criteria determine which of the various described device assisted agent functions should be executed in protected DAS partition 114 to strengthen the service control integrity for the system.

**[0035]** In some embodiments, the device operating system provides for the protected DAS partition 114 in addition to conventional security features available in the operating system. In some embodiments, the protected DAS partition 114 provides an execution partition with increased program execution protection in which, for example, service measurement and/or service control programs (agents) can execute in a mode that provides for higher access control integrity (e.g., proper service usage reporting and/or service measurement and/or service control system operation with increased protection from attacks, errors, malware, etc.). In some

embodiments, a hardware assisted secure execution partition provides for increased program execution protection for device assisted service agent functions.

**[0036]** In some embodiments, a service control link (e.g., host service control link 118 via host secure channel 150 to network service control link 152) is used for communication between the device assisted service agents and a service controller 122. In some embodiments, the service control link is a secure link (e.g., an encrypted communications link). In some embodiments, an encrypted secure control link can be implemented over the higher layers of the network stack (e.g., TCP, HTTP, TLS, etc.), and, in some embodiments, the encrypted link can be implemented over lower layers in the network stack, such as the IP layer or the access network layers (e.g., the WWAN device management channels or signaling layers). In some embodiments, service control link security is provided at least in part by encrypting link traffic between the device and the service controller 122. In some embodiments, service control link security is provided at least in part by running the service control link device side program agents in the protected DAS partition 114. In some embodiments, service control link security is achieved at least in part by restricting access to the service control link to certain device assisted service agents that are allowed to communicate with the service controller 122. In some embodiments, the agents that are allowed to communicate with the service control link perform such communications using encrypted communications. In some embodiments, the encrypted communications is accomplished with a secure inter-agent communication bus on the device. In some embodiments, the only mechanism for modifying the configuration of the operation, execution code, execution instructions and/or settings of certain device assisted service processor agents executing in the protected DAS partition 114 is through the service control link. In some embodiments, the only mechanism for modifying any program elements executing inside the protected DAS partition 114 is through the service control link so that only the service controller 122 may modify the operation or service policy settings for the agents located in the service measurement and/or service control execution partition.

**[0037]** As shown in Figure 1, various server functions within the service controller 122 are provided. In some embodiments, a service history server 158 collects service usage measures from one or more of the device DAS agents and/or from various sources of potential network based service usage databases, such as the access network service usage 142 (e.g., carrier

charging data record (CDR) systems), private network service usage 144 (e.g., MVNO or enterprise network service usage accounting system), and/or billing, mediation service usage log, reconciliation 148 (e.g., service provider billing or mediation system). In some embodiments, an access control integrity server 156 is used to compare various access control verification checks to ensure that the device assisted service agents have not been compromised. The various embodiments used in the access control integrity server 156 to perform these integrity checks are described with respect to various embodiments. Some embodiments include comparing device based service usage measures versus the service usage that should result if the desired service policy were properly implemented, comparing device based service usage measures versus the service usage that should result if the desired service policy were properly implemented with device based service usage measures that are executing in the protected DAS partition 114 and/or the modem execution partition 124, comparing network based service usage measures versus the service usage that should result if the desired service policy were properly implemented, and comparing network based service usage measures with device based service usage measures. In some embodiments, a policy control server 154 stores policy settings for the various service plans that can be implemented on the device, and communicates the appropriate policy settings to the appropriate device DAS agents.

**[0038]** In some embodiments, the service controller 122 has secure access to service measures, service control settings, software images, software security state(s), and/or other settings/functions, for example, by virtue of the hardware enhanced execution partition and the secure channel into the protected DAS partition 114. For example, the host secure channel 150 can be encrypted employing keys that are public/private or point to point private. Also, other link security, for example, can be implemented as described herein. For example, servers can ensure that the link remains authenticated and information is validated. For example, the service controller can perform one or more of the following verification techniques: compare the monitored service usage versus the policy, compare the monitored service usage versus other service usage measures and/or combined with various other network service usage measures.

**[0039]** In some embodiments, the protected DAS partition 114 includes a host service control link 118 as shown in Figure 1 that works in combination, that is, in communication with a network service control link 152 to send and receive secure messages between the service

controller and the host via a host secure channel 150. In some embodiments, the protected DAS partition 114 only accepts new program images from the service controller 122 and not from local programs or disks. In some embodiments, the protected DAS partition 114 cannot communicate with other applications and/or kernel programs. In some embodiments, the protected DAS partition 114 can also communicate with other applications and/or kernel programs but only to gather information or to set settings. In some embodiments, the protected DAS partition 114 can also communicate with other applications and/or kernel programs but only through a restricted encrypted communication bus that restricts outside program access to protected programs or agent functions, and can also restrict the agents inside of the protected partition from accepting unauthorized information or code modifications from programs outside the protected partition. Various other security techniques can be provided for the DAS execution environments as will be apparent to one of ordinary skill in the art in view of the embodiments described herein.

**[0040]** In some embodiments, the protected DAS partition 114 is created by employing CPU or APU hardware security features in addition to or in alternative to other software security features (e.g., virtual execution partitions) that can be provided by the operating system and/or other software. In some embodiments, the host hardware security features are provided with the operating system secure kernel operating modes. In some embodiments, the host hardware security features used for secure device assisted service execution partition operation are independent of the operating system kernel (e.g., implemented in secure program partitions in a separate secure program area not directly controlled by the OS and/or software that does not have access to the partitions).

**[0041]** In some embodiments, the hardware security features that support the protected DAS partition 114 include preventing other elements on the device from writing and/or reading certain memory areas reserved for device assisted service agents and/or control link functions. In some embodiments, this memory protection function is accomplished by locating the memory in a secure hardware partition that cannot be accessed by unauthorized device program elements (e.g., a separate bank of isolated memory space within the host CPU). In some embodiments, this memory protection function includes encrypting traffic to and from memory so that only authorized device program elements posses the counterpart encryption capability to access the

memory. In some embodiments, the mechanism to access device assisted service agent memory and/or certain data elements is restricted to authorized device assisted service agents and/or the service controller via the service control link so that unauthorized program elements on the device cannot alter the device assisted service agent code and/or operation.

**[0042]** In some embodiments, the hardware security features that support the protected DAS partition 114 includes preventing unauthorized elements on the device from accessing the protected storage and/or file storage (e.g., "protected storage," such as disk storage, non-volatile memory, embedded non-volatile memory, such as NVRAM, flash or NVROM, securely embedded non-volatile memory, and/or other types of storage) that is used to store the device assisted service agent programs. In some embodiments, this protected storage is maintained within the secure hardware partitions that also execute one or more of the device assisted service agents so that only authorized device assisted service agents have access to the storage locations. In some embodiments, the images that are stored in such protected file storage must be properly encrypted and signed for a boot loader to authorize loading the device assisted service agent programs into execution memory, and in some embodiments, if the images are not properly signed then an access control integrity error is generated and/or the program is not loaded. In some embodiments, such properly signed DAS images can only be obtained from the service controller. In some embodiments, such DAS images can only be loaded into protected file storage by the service controller. In some embodiments, the hardware security features that prevent unauthorized elements on the device from accessing the protected file storage include encrypting all traffic to and from the secure storage so that only authorized device program elements possess the counterpart encryption capability to access the storage. In some embodiments, access or access rights to re-program a device assisted service agent program store is restricted to the service controller via the service control link so that unauthorized program elements on the device are not authorized to alter the device assisted service agent code and/or operation.

**[0043]** In some embodiments, the hardware security features that protect device assisted service agent storage include a protected DAS partition in which an access control integrity agent function is isolated from other device program elements, and a secure service control link is also isolated in a similar manner, and the access control integrity agent scans the execution memory,

data memory and/or file storage used by one or more device assisted services agents to measure and/or control services. In some embodiments, the purpose of the scan is to detect changes to the device assisted service agent code and/or data. In some embodiments, the purpose of the scan is to detect other unauthorized program elements or data that may be present in reserved or protected areas used for device assisted service agent execution. In some embodiments, reports of such scan audits are reported over the service control link to the service controller for further processing by use of cloud based resources to identify access control integrity violations. In some embodiments, the access control integrity agent functions include one or more of hashing other device assisted security agents, querying other device assisted security agents, observing the operation of other device assisted security agents or monitoring service measures and then either evaluating the results locally on the device to determine if they are within pre-defined allowable parameters or sending at least some of the results to the service controller for further analysis via the service control link. In some embodiments, the scan audits are compared with earlier versions of the scans to compare code configuration or operational characteristics. In some embodiments, the scan audits are compared against known databases for the code or operational characteristics that should be present in the DAS agents.

**[0044]** In some embodiments, an access control integrity agent, or a new version of the access control integrity agent can be downloaded by the service controller over the secure service control link. For example, this technique provides for a real time assessment of device service control security state as described above in the event that corruption or compromise of the secure device assisted service agent(s) has occurred. In some embodiments, the access control integrity agent that is downloaded can have a different configuration and/or operation than any agent previously loaded onto the device so that it is difficult or impossible for a hacker or malware to spoof the operation of the agent in a short period of time. For example, by requiring the agent to report security assessments back to the server in a period of time that is typically less than what is required to spoof the agent, the agent will either report back an accurate assessment of device status or will be blocked by a hacker or malware, and both of these conditions can provide the information required to take action if the device assisted services system has been corrupted or compromised.

**[0045]** In some embodiments, the protected DAS partition and/or the modem execution partition can be used to securely store some or all of the device credentials that are used for one or more of device group association, activation, authorization to the access network and/or the DAS network, service level, and service usage accounting and/or billing.

**[0046]** In some embodiments, the modem subsystem also includes DAS elements that strengthen the access control integrity of the DAS system. As shown in Figure 1, one or more modems can include, in some embodiments, DAS agent functions labeled modem partition DAS agents 126. The modem execution partition 124 of the modem sub system #1 (125) of the modem execution partition 124 includes modem partition DAS agents 126 in communication (e.g., secure communication, such as using encrypted communications) with a modem 128 and a modem service control link 130, which is in communication with the network service control link 152 via the modem secure channel #1 (132), as shown. Also, the modem 128 is in communication (e.g., secure communication, such as using encrypted communications) with the access network #1 (136), which is in communication with the access network service usage 142 and the Internet 140, which is in communication with a private network 146, which is in communication with the private network service usage 144, as shown.

**[0047]** Example embodiments for DAS agent functions that execute in the modem execution partition include modem encryption and modem service usage measures. In other embodiments, the modem execution partition can also include higher level DAS agent functions, such as stack traffic classification, stack manipulation, access control, and/or traffic control. For example, the modem execution partition can also include a full service processor that is fully capable of managing all aspects of service usage measurement and/or service control. It will now be apparent to one of ordinary skill in the art that the modem execution partition can employ a number of the service security embodiments described in the context of the protected DAS partition, for example, to enhance the service integrity of the DAS system. For example, the DAS agents on the modem can be stored in an encrypted and signed format on non-volatile (NV) memory on the modem that is only accessible by the network service control link or by a local secure control link from the protected DAS partition to the modem execution partition. As shown in Figure 1, a separate secure modem control channel (e.g., modem secure channel #1 (132) through modem secure channel #N (134)) that is distinct from the host secure control

channel 150 is provided. This separate modem control channel can either be implemented over the higher network layers of the device or over the lower access network layer so that special access to access network resources is required to even connect to the modem DAS agents 126 thereby further enhancing service control related security.

**[0048]** In some embodiments, the protected DAS partition provides for performing the DAS agent functions required for parental controls, enterprise WWAN management controls or roaming controls, and/or usage reporting in the protected execution space. In view of the DAS embodiments described herein, it will now be apparent to one of ordinary skill in the art how to implement such protected controls for these various and other application scenarios.

**[0049]** In some embodiments, a protected DAS partition provides for performing a virtual machine (VM) on top of a secure machine. The device application OS that is accessible by software that can be installed without special permissions can be isolated from the secure hardware and/or OS that is running under the VM. Using these techniques, malware can be "cocooned in" on the VM OS rather than "walled out" as discussed with respect to various embodiments described herein.

**[0050]** In some embodiments, communication between program/functional elements outside of the protected DAS partition to DAS agents inside the protected DAS partition is controlled by a secure encrypted channel. In some embodiments, only programs/functions that have access to communicate with DAS agents are allowed to do so, and, in some embodiments, even these outside programs are not allowed to modify the DAS agent configuration, only to report information and/or receive information.

**[0051]** For example, various embodiments can be used to connect to multiple access networks through multiple modems, with each modem potentially being associated with a different set of DAS service policies corresponding to the different types of access networks supported. In some embodiments, such as for 3G/4G modems, WWAN/WLAN modems, and various other multiple modem embodiments, the multiple modems can also be provided on the same multi-mode modem subsystem rather than on different modem subsystems.

**[0052]** In some embodiments, the various techniques and embodiments described herein can be readily applied to intermediate networking devices as will now be apparent to one of ordinary skill in the art. For example, an intermediate networking device can includes some or all of the DAS agents for managing, controlling, and/or measuring service usage for one or more devices in communication with a wireless network via the intermediate networking device, in which the DAS agents can be executed in secure execution environments or secure execution partitions using the various techniques described herein. In some embodiments, intermediate networking devices include, for example, WWAN/WLAN bridges, routers and gateways, cell phones with WWAN/WLAN or WWAN/Bluetooth, WWAN/LAN or WWAN/WPAN capabilities, femto cells, back up cards for wired access routers, and other forms/types of intermediate networking devices.

**[0053]** **Figure 2** illustrates another secure execution environment 200 for device assisted services in accordance with some embodiments. In particular, Figure 2 illustrates an embodiment in which DAS agents do not actually replace the OS network stack elements, but instead one or more DAS agents include device driver programs that interface into the network stack and pass (e.g., securely communicate) traffic information or actual traffic back and forth with the stack. These device driver interface constructs are labeled OS driver framework and interface 208 as shown in Figure 2. Example OS system constructs that provide for this type of architecture for DAS agents include Windows NDIS and/or TDI drivers, Windows Filter Platform (WFP), Berkeley Packet Filter, ipfw (e.g., a BSD packet filter that can be used for various OSs, such as Unix, Linux, MAC OS), and/or other platforms/programs performing these or similar functions. While these OS stack options are not secure in themselves, if the drivers that interface with them are secured as illustrated in Figure 2 by executing the drivers in the protected DAS partition 214, then higher overall access control integrity/security levels can be achieved.

**[0054]** As shown in Figure 2, the service measurement and/or policy control drivers 210 executed in the protected DAS partition 214 represent the DAS drivers that interface to the OS stack device driver interface constructs labeled OS driver framework and interface 208 executed in the kernel execution partition 212, which are in communication with/interface with OS Stack API(s) 207. As also shown, applications, such as applications 106A through 106C execute in the

application execution partition 202. In some embodiments, service access control integrity is further enhanced by placing additional measurement points outside of the network stack, so that, for example, if the network stack service usage reporting is hacked, corrupted, and/or compromised, there is a secure additional or back-up service measure located on the device and/or in the network (e.g., modem agent 226 as shown in Figure, which provides a service measurement point in the modem for measuring service usage by the device, and as shown also provides for secure communication with the modem agent 226 using modem encryption 225). For example, the service measure provided by the modem agent 226, modem encryption 225, and/or modem bus 120 functions shown in Figure 2 can be executed in a protected partition (e.g., modem execution partition 124 as shown in Figure 2 can be implemented as a secure or protected partition using the various techniques described herein).

**[0055]** **Figure 3** illustrates another secure execution environment 300 for device assisted services in accordance with some embodiments. As shown, some stack elements are executed in the kernel execution partition 312 and some stack elements are executed in the protected DAS execution partition 314. In some embodiments, the DAS agents 104 executed in the application execution partition 302 are directly monitoring and/or controlling stack traffic by intercepting it and imposing additional traffic measurement and/or filtering. Examples of such techniques are described herein with respect to various embodiments. As shown in Figure 3, the network stack elements 308 are the OS stack elements that reside in the kernel execution partition 312 and the protected DAS network stack elements 310 are the stack elements that reside in protected DAS execution partition 314. For example, as some or potentially all of the stack network traffic processing resides in the protected DAS execution partition 314, a high level of service control integrity can be maintained using these techniques. For example, the modem bus driver 121 can be executed in a secure execution partition, such as modem execution partition 324, which can be implemented as a secure execution partition using the various techniques described herein, or the modem bus driver 121 can be executed in the protected DAS execution partition 314, so that unauthorized programs can be blocked from accessing the access network through the modem.

**[0056]** In some embodiments, the entire stack is executed in the protected DAS execution partition 314 with only a stack API executing in kernel execution partition 312. Various other embodiments involve implementing a minimum (e.g., in terms of a number of agents and/or

functionality) in the protected DAS execution partition 314 required to secure a service measure that can be used to confirm the integrity of the service policy implementation (e.g., as described with respect to various other embodiments disclosed herein). As will now be apparent to one of ordinary skill in the art, various combinations of stack processing functions can be implemented in a secure host execution partition to strengthen the service measurement and/or service control integrity of the DAS system using the techniques and/or similar techniques to the various techniques described herein.

**[0057]** In some embodiments, the stack elements implemented in the protected DAS execution partition can include stack API, sockets layer, TCP, UDP, service measurements at one or more points in the stack, IP layer processing, VPN/IPSEC, PPP, access control, traffic classification, traffic queuing, traffic routing, traffic QOS, traffic demand reporting to QOS allocation servers, traffic statistics reporting to the QOS servers, traffic QOS reservation requests including by traffic type or app type or service priority to the servers, traffic throttling, traffic statistics gathering, traffic QOS priority identification, modem drivers, modem data encryption, and/or other stack element functionality or features.

**[0058]** In some embodiments, the above discussed service control mechanisms are controlled by policy commands received over the service control link from the servers or other authorized network elements. In some embodiments, the device also reports usage measures to servers or other authorized network elements. In some embodiments, the device also reports QOS demand to the servers or other authorized network elements and/or accepts QOS instructions from the servers or other authorized network elements. In some embodiments, the device reports traffic statistics, projected traffic demand, application usage, projected QOS demand can all be reported to the servers or other authorized network elements for the purpose of provisioning the right amount of data bandwidth and traffic priority to the device, and the servers or other authorized network elements aggregate such reports from many different devices to project needed allocations across the entire network and make global bearer channel level or base station level decisions bearer channel allocation and bearer channel QOS allocation decisions, which can also be tied into a bearer channel provisioning, or bearer channel QOS provisioning apparatus or other authorized network elements located in the access network.

**[0059]** For example, as will now be apparent to one of ordinary skill in the art in view of the various embodiments described herein, additional security measures, can be added in some embodiments to augment the secure service partitioning, including, for example, access control integrity checks. For example, in addition to the service control policy instructions that can be received from the servers or other authorized network elements, an intermediate policy control agent can be present to make additional higher level decisions on how instantaneous policy should be implemented.

**[0060]** As shown in Figure 3, the modem control link, shown as modem local channel 330, provides a link from local connection to the host service control link 118, which in turn connects through the host secure channel 150 to the service controller 152. This communication channel can also be implemented or configured to provide for encrypted communication and, in some embodiments, can be used as an alternative to the direct connection from the modem service control link to the network service control link as disclosed with respect to other figures and various embodiments as described herein.

**[0061]** As shown in Figure 3, the final stack elements that feed or communicate with the modem bus driver 121 are the protected DAS network stack elements 310 located in the protected DAS execution partition 314 (illustrated as a solid line in Figure 3), or, in some embodiments, can be the network stack elements 308 located in the kernel execution partition 312 (illustrated as a dashed line in Figure 3). In some embodiments, these final stack elements feed or communicate with the modem subsystem 125. In some embodiments, the modem subsystem 125 includes an encrypted link so that the stack elements 310 in the protected DAS execution partition 314 can communicate with the modem 128 but other software programs or hardware elements cannot, for example, thereby preventing the service measures and/or controls from being inappropriately bypassed or otherwise comprised. For example and as similarly discussed above, the modem subsystem 125, for example, can include its own the protected execution partition using various techniques described herein. The modem protected execution partition, for example, can also include a service measure (e.g., modem agent 226 can provide such a service measurement point in the modem subsystem 125, as similarly described above with respect to Figure 2) to increase service control integrity verification as depicted by service measure. The modem service measure can be included in protected execution partition that can

only be accessed by the service controller 122 by way of the modem local channel 330, or the modem service measure can only be accessed by another DAS agent 310 in protected execution partition 314. In some embodiments, the modem local channel 330 is implemented as a secure channel (e.g., an encrypted communication channel between the modem service control link 130 and the host service control link 118). As described herein, the modem driver can reside in protected service execution environment, or the modem traffic can be encrypted within service execution environment. For example, the encryption settings can be controlled by various secure control servers.

**[0062]** **Figure 4** illustrates another secure execution environment 400 for device assisted services in accordance with some embodiments. In particular, Figure 4 illustrates a direct stack manipulation option performed by the DAS agents executed in the protected DAS execution partition 414, including, as shown, an app(lication) identify agent 420, an access control integrity agent 422, a policy control agent 424, a policy implementation agent 426, a service measure/service monitoring agent 428, a modem encryption agent 430, and a bus driver 432. For example, the policy implementation agent 426 performs access control and/or traffic shaping according a set of service control policies. The service control policies, for example, can be set by the service controller 122 or by the service controller 122 in coordination with the policy control agent 422. As shown the app identify agent 420 is in communication with the various applications 106A through 106C executed in the application execution partition 402. As also shown, the various applications 106A through 106C executed in the application execution partition 402 are in communication with the OS stack and/or stack API(s) 408 executed in the kernel execution partition 412.

**[0063]** In some embodiments, the protected service measure agent 428, the modem encryption agent 430, the modem driver agent 432, the application identifier agent 420, the access control integrity agent 422, and the policy control agent 424 are all implemented in protected DAS partition 414, as shown. In some embodiments, as will now be apparent to one of ordinary skill in the art, a subset of these functions can be implemented in a protected execution partition, such as the protected DAS partition, in various circumstances.

**[0064]** Figure 4 also similarly shows various embodiments that are available for network based service usage measures and interfacing to the mediation and billing systems, and it should be understood that any or all of the embodiments and figures can be employed in the context of carrier networks, MVNOs, private networks, or open networks supporting enterprise IT manger controls, parental controls, multi-network controls, and/or roaming controls.

**[0065]** **Figure 5** illustrates another secure execution environment 500 for device assisted services in accordance with some embodiments. In particular, Figure 5 is similar to that Figure 4 except that Figure 5 illustrates a modem service control link 132 that is connected directly to the service controller 122 via the network service control link 152 (e.g., via a modem secure channel). In some embodiments, a modem control link for DAS is established locally on the device or through an entirely different control channel, which, in some embodiments, provides enhanced security as discussed herein (e.g., it is very difficult to hack a service usage measure or service control that cannot be accessed on the device).

**[0066]** **Figure 6** illustrates another secure execution environment 600 for device assisted services in accordance with some embodiments. In particular, Figure 6 illustrates a policy implementation agent 616 that includes the entire networking stack running in protected execution partition 614 and an OS stack API 608 that includes an application identifying function 620 in the kernel execution partition 612.

**[0067]** **Figure 7** illustrates another secure execution environment 700 for device assisted services in accordance with some embodiments. In particular, Figure 7 illustrates DAS agents that do not replace the OS network stack elements, but instead one or more DAS agents are comprised of device driver programs that interface into the network stack and pass traffic information or actual traffic back and forth with the stack. These device driver interface constructs are labeled OS driver framework and interface 722 in Figure 7 as similarly shown in and described with respect to Figure 2, along with OS stack API 708, which includes application identifier function 720 as similarly discussed above with respect to Figure 6, and are executed in kernel execution partition 712. Also, as shown, application partition DAS agents 104 are executed in application execution partition 702. The main difference between the embodiment in Figure 7 and that shown in and described with respect to Figure 2 is that the service measure

agent 428, modem encryption agent 430, and modem driver agent 432 are executed in the protected DAS partition 714, as shown in Figure 7. For example, this provides for enhanced service control security as described herein with respect to various embodiments.

**[0068]** **Figure 8** illustrates another secure execution environment 800 for device assisted services in accordance with some embodiments. In particular, Figure 8 illustrates a more simplified embodiment that is similar to that of Figure 7. In Figure 8, only an access control integrity agent 422 and a service measure 428 are executed in protected DAS partition 814, and the bus driver 432 and the service measurement and/or policy control drivers 210 are executed in the kernel execution partition 712. This embodiment illustrates that provided that at least one protected service measure is provided on the device, then the DAS service control integrity can be very high. For example, if it is not possible to access the program code or control traffic for the service measure agent 428, and the host service control link 118 except through the encrypted control channel from the service controller 122, then this simplified configuration can be almost as secure as that possible with network based service measures. It will now be apparent to one of ordinary skill in the art that this technique similarly applies to a service measure and control link similarly implemented in a protected modem execution partition 324. In some embodiments, the access control integrity agent 422 provides additional security, for example, in the event that the protected DAS partition 814 is breached or compromised.

**[0069]** **Figure 9** illustrates another secure execution environment 900 for device assisted services in accordance with some embodiments. In particular, Figure 9 illustrates an embodiment similar to that of Figure 8 except that, in particular, in addition to the service measure being executed in protected DAS partition 914, the modem encryption agent 430 is also implemented in/executed in the protected DAS partition 914. For example, this prevents unauthorized software from defeating the service measurements and/or service controls by going around the network stack directly to the modem.

**[0070]** **Figure 10** illustrates another secure execution environment 1000 for device assisted services in accordance with some embodiments. In particular, Figure 10 illustrates an embodiment similar to that of Figure 9 except that, in particular, there are additional app partition DAS agents 104 executing in the application execution partition 702. For example, this

illustrates that some DAS agents can be implemented in application space (e.g., UI agent, policy control agent, and various other DAS agents as described herein) while still maintaining a high level of service measurement and/or control security as long as there are a few key measures and/or controls implemented in protected execution partitions using the various techniques described herein.

**[0071]** **Figure 11** illustrates another secure execution environment 1100 for device assisted services in accordance with some embodiments. In particular, Figure 11 illustrates how the server cloud can be assisted by the on board access control integrity agent to detect tampering with other service measurement(s) and/or control agent(s), or to protect the service measurement and/or control system from being attacked by malware and/or otherwise comprised. As shown, the access control integrity agent 422 executes inside the protected DAS partition 1114 and is in communication with file storage 1130 (e.g., for persistently maintaining device status and/or other settings or status or monitoring information). The access control integrity agent 422 performs the various access control integrity check functions as, for example, described herein with respect to various embodiments, and, in some embodiments, in coordination with the servers over the secure control channel (e.g., host secure channel 150). In some embodiments, the access control integrity agent 422 can send the service controller 122 information about the other service measurements and/or control agents so that the service controller 122 can determine if the agents are working properly or have been tampered with or otherwise compromised. For example, such information can include sections of code, hashes, code segments, code variations from a previous image, code variations from a historical image, responses to queries, checksums, observations of operating behavior or patterns, service usage, policy implementation behavior, and/or other information that may be indicative of tampering, corruption, and/or a compromise of any of the device agents/measures. In some embodiments, the access control integrity agent 422 checks the operating environment for signs of malware signatures, or sends application and/or driver information or other information about the operating environments to the servers for further processing to detect malware. In some embodiments, the access control integrity agent 422 performs basic operations on protected DAS partition memory, kernel execution partition memory areas, application execution partition memory areas, on disk storage areas or on other file storage areas to detect known malware hashes or signatures, etc., or the access control integrity agent 422 can send the hashes to the

servers for comparison against malware databases (e.g., to compare against signatures for known malware or for further behavioral based or other security/malware detection techniques).

**[0072]** In some embodiments, the DAS system is implemented in a manner that is robust to losses in service control link (e.g., coverage outages on a WWAN link or loss of connection on a wired link). In some embodiments, the DAS system to be implemented in a manner that is robust to one or more server elements in the service controller going offline or failing for any reason. The following embodiments facilitate these techniques, as described below.

**[0073]** In some embodiments, it is advantageous for one or more of the device assisted service agents to maintain a record of the service usage reports and/or other reporting that is provided to the service controller regarding device service control state (e.g., present service plan settings, current service usage policy settings, current user preference settings, current DAS settings, current encrypted control channel and/or local encrypted communication channel key information, current DAS agent status reports, current DAS agent security state reports, current ambient service usage and/or transaction records, current service control integrity threat reports, user status information, device status information, application status information, device location, device QOS state, and/or other state and/or settings information). In addition to such information that exists on the device and is reported to the service controller, additional service information can be derived and recorded in the service controller, such as information received from outside the device and/or analysis of the device reported information (e.g., network based service usage measures, analysis of device service usage, comparison of device reports with other information, analysis of access control integrity agent reports, information received from roaming networks, information input to the service controller from parental control terminals, enterprise control terminals, virtual service provider control terminals, access network authorization information, service integrity violation level, and many other types of information used to properly measure and/or control the device services). For example, the information reported from the device and received or derived outside the device that is required to adequately define the actions needed from the service controller to maintain proper DAS system operation is sometimes referred to herein as the "device service state."

**[0074]** In some embodiments, the service controller functions are highly scalable and can be executed on a number of hardware and software platforms (e.g., different virtual machines in a server, different servers in a data center, or different servers located in different data centers). For example, in such embodiments the service controller can be designed so that the programs that execute the various service controller server functions can derive all of the information necessary to properly manage the device at any moment in time by knowing past device service state and current service state that adequately define the next set of actions the service controller needs to implement to properly maintain the DAS system operation. By designing the system in this way, if the server that is running the service controller server functions for any given device in question were to go down or become disconnected from the device, then another server could later resume proper operation of the DAS system by assigning another service controller server function to the device and recovering or restoring the necessary past device service state and the necessary current device service state.

**[0075]** For example, this can be accomplished in some embodiments as described below. The service controller saves the current device service state into a common database (e.g., which can be centralized or distributed) that is available to all service controller server functions. The device service state is saved each time the device communicates with the service controller, or at regular time intervals, or a combination of both. The device retains its current and past service state reports even after they are reported at least until the service controller sends the device a message confirming that the service controller has saved a given device service state. Once the device receives this save confirmation for a given device state report then it is no longer required to retain that particular device state report once the device has no further use for it. In this manner, if a service controller server function goes down then a save confirmation for one or more reported device states is not transmitted to the device by the service controller, and the device can retain that report. A server load balancer detects that a given service controller server function has gone down, looks up the devices that were being controlled by that service controller server function, finds that the device in question was one of those devices and re-assigns a new service controller server function (either in the same data center or in another data center) to control the device in question. The newly assigned service controller server function then recovers all past device states that were recorded in the service controller database and are required to properly manage the DAS system, and then asks the device to transmit or re-transmit

all device state reports that were not saved in the service controller database. Once the device transmits or re-transmits the requested information, the newly assigned service controller function then has the information it needs to properly manage the DAS system, it saves all the reported device state information, and then sends save confirmations to the device so that the device need no longer retain the older service state reports. The newly assigned service controller server function can then resume the DAS system operation with a set of actions that are identical or very similar to the actions that would have been taken by the original service controller server function if it had not gone down. One of ordinary skill in the art will now appreciate that the above techniques can also be used to accommodate temporary losses in the connection between the device and the service controller. For example, such techniques provide for a highly scalable and robust approach to implement a distributed service controller across multiple data centers for reliable service redundancy. In some embodiments, the past device service state information is saved in the protected DAS execution partition and/or the modem execution partition, for example, so that it is protected from corruption.

**[0076]** Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

**[0077]** WHAT IS CLAIMED IS:

CLAIMS

1. A system, comprising:

a processor of a communications device configured to:

implement a service profile executed at least in part in a secure execution environment for assisting control of the communications device use of a service on a wireless network, wherein the service profile includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service on the wireless network;

monitor use of the service based on the service profile; and

verify the use of the service based on the monitored use of the service;

a memory of the communications device coupled to the processor and configured to provide the processor with instructions.

2. The system recited in claim 1, wherein the use of the service is verified based at least in part on device based service usage information.

3. The system recited in claim 1, wherein the communications device is a mobile communications device or an intermediate networking device, and the service includes one or more Internet based services.

4. The system recited in claim 1, wherein the communications device includes a modem, and the processor is located in the modem.

5. The system recited in claim 1, wherein the communications device is a mobile communications device, and the service includes one or more Internet based services, and wherein the mobile communications device includes one or more of the following: a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, a tablet, and a home networking system.

6. The system recited in claim 1, wherein the service plan allows for access to the service with service capabilities that are controlled based on one or more of the following: period of time, network address, service type, content type, application type, bandwidth, and data usage.

7. The system recited in claim 1, wherein the service policy settings include one or more of the following: access control settings, traffic control settings, billing system settings, user notification with acknowledgement settings, user notification with synchronized service usage information, user privacy settings, user preference settings, authentication settings, admission control settings, application access settings, content access settings, transaction settings, and network or device management communication settings.

8. The system recited in claim 1, wherein the secure execution environment includes a protected device assisted service execution partition.

9. The system recited in claim 1, wherein the secure execution environment includes a protected device assisted service execution partition, and wherein the protected device assisted service execution partition is implemented at least in part as a hardware partition.

10. The system recited in claim 1, wherein the secure execution environment includes a protected device assisted service execution partition, and wherein the protected device assisted service execution partition is implemented at least in part as a software partition.

11. The system recited in claim 1, wherein the secure execution environment includes a protected device assisted service execution partition, and wherein the protected device assisted service execution partition is implemented at least in part in a virtual machine executed on the processor.

12. The system recited in claim 1, wherein the secure execution environment includes a protected device assisted service execution partition, and the processor is further configured to:

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition are in communication with a server executing a service controller.

13. The system recited in claim 1, wherein the secure execution environment includes a protected device assisted service execution partition, and the processor is further configured to:

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition include a device agent for providing a service usage measure.

14. The system recited in claim 1, wherein the secure execution environment includes a protected device assisted service execution partition, and the processor is further configured to:

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition are in secure communication with a server executing a service controller, and wherein the secure communication with the server executing the service controller includes encrypted communications.

15. The system recited in claim 1, wherein the communications device includes a modem, and the processor is located in the modem, and wherein the secure execution environment includes a secure modem execution partition that is implemented using a hardware and/or software partition, and wherein the processor is further configured to:

execute one or more device assisted service agents in the secure modem execution partition, wherein the device assisted service agents executed in the secure modem execution partition are in communication with a server executing a service controller.

16. The system recited in claim 1, wherein the communications device includes a modem, and the processor is located in the modem, and wherein the secure execution environment includes a secure modem execution partition that is implemented using a hardware and/or software partition, and wherein the processor is further configured to:

execute one or more device assisted service agents in the secure modem execution partition, wherein the device assisted service agents executed in the secure modem execution partition are in secure communication with a server executing a service controller, and wherein the secure communication with the server executing the service controller includes encrypted communications.

17. The system recited in claim 1, wherein the communications device includes a modem, and the processor is located in the modem, and wherein the secure execution environment includes a secure modem execution partition that is implemented using a hardware and/or software partition, and wherein the processor is further configured to:

execute one or more device assisted service agents in the secure modem execution partition, wherein one or more device assisted service agents executed in the secure modem execution partition include a modem agent for providing service usage measure.

18. The system recited in claim 1, wherein the processor of the communications device is further configured to:

execute one or more device assisted service agents in a kernel execution partition; and

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition are in communication with a server executing a service controller.

19. The system recited in claim 1, wherein the processor of the communications device is further configured to:

execute one or more device assisted service agents in an application execution partition;

execute one or more device assisted service agents in a kernel execution partition; and

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition are in communication with a server executing a service controller.

20. The system recited in claim 1, wherein the processor of the communications device is further configured to:

execute one or more device assisted service agents in an application execution partition;

execute one or more device assisted service agents in a kernel execution partition;

execute one or more device assisted service agents in a modem execution partition; and

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition are in communication with a server executing a service controller.

21. The system recited in claim 1, wherein the processor of the communications device is further configured to:

execute one or more device assisted service agents in an application execution partition;

execute one or more device assisted service agents in a kernel execution partition;

execute one or more device assisted service agents in a modem execution partition; and

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition are in communication with a server executing a service controller, and wherein the one or more device assisted service agents executed in the protected device assisted service execution partition include one or more of the following: an application identifier agent, an access control integrity agent, a policy control agent, a policy implementation agent, and a service usage measure agent.

22. The system recited in claim 1, wherein the processor of the communications device is further configured to:

execute one or more device assisted service agents in an application execution partition;

execute one or more device assisted service agents in a kernel execution partition;

execute one or more device assisted service agents in a modem execution partition, wherein the modem execution partition is in communication with the protected device assisted execution partition using a modem local channel; and

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition are in communication with a server executing a service controller, and wherein the one or more device assisted service agents executed in the protected device assisted service execution partition include one or more of the following: an application identifier agent, an access control integrity agent, a policy control agent, a policy implementation agent, and a service usage measure agent.

23. The system recited in claim 1, wherein the processor of the communications device is further configured to:

execute one or more device assisted service agents in an application execution partition;

execute one or more device assisted service agents in a kernel execution partition;

execute one or more device assisted service agents in a modem execution partition, wherein the modem execution partition is in communication with the protected device assisted execution partition using a modem local channel, and wherein the one or more device assisted service agents in the modem execution partition include a service usage measure agent; and

execute one or more device assisted service agents in the protected device assisted service execution partition, wherein the one or more device assisted service agents executed in the protected device assisted service execution partition in communication with a server executing a service controller, and wherein the one or more device assisted service agents executed in the protected device assisted service execution partition include one or more of the following: an application identifier agent, an access control integrity agent, a policy control agent, a policy implementation agent, and a service usage measure agent.

24. A method, comprising:

implementing a service profile executed at least in part in a secure execution environment of a processor of a communications device for assisting control of the communications device use of a service on a wireless network, wherein the service profile includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service on the wireless network;

monitoring use of the service based on the service profile; and

verifying the use of the service based on the monitored use of the service.

25. A computer program product, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

implementing a service profile executed at least in part in a secure execution environment of a processor of a communications device for assisting control of the communications device use of a service on a wireless network, wherein the service profile includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service on the wireless network;

monitoring use of the service based on the service profile; and

verifying the use of the service based on the monitored use of the service.

# SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

## ABSTRACT OF THE DISCLOSURE

**[0078]** Security techniques for device assisted services are provided. In some embodiments, secure service measurement and/or control execution partition is provided. In some embodiments, implementing a service profile executed at least in part in a secure execution environment of a processor of a communications device for assisting control of the communications device use of a service on a wireless network, in which the service profile includes a plurality of service policy settings, and wherein the service profile is associated with a service plan that provides for access to the service on the wireless network; monitoring use of the service based on the service profile; and verifying the use of the service based on the monitored use of the service.

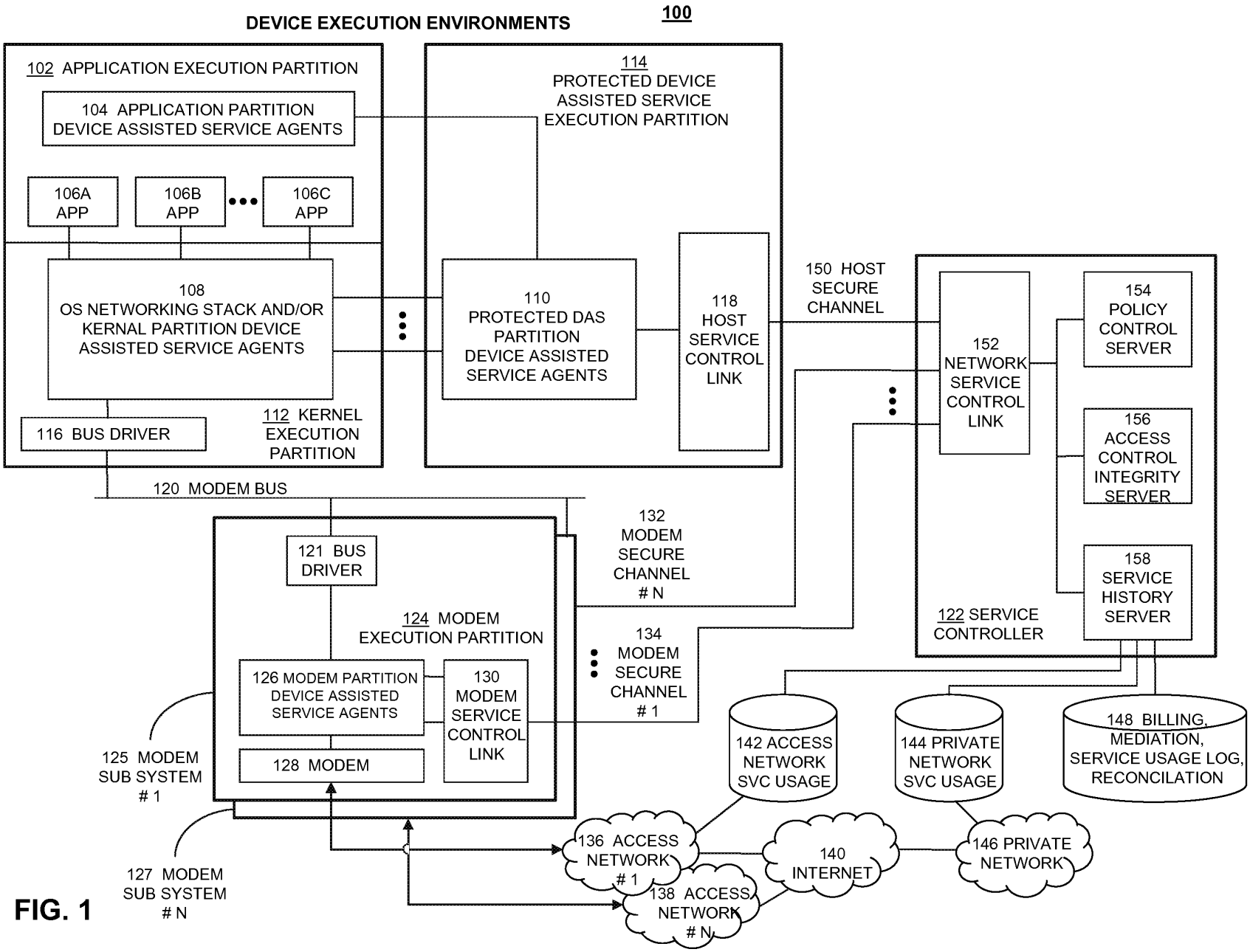

DEVICE EXECUTION ENVIRONMENTS
100
102 APPLICATION EXECUTION PARTITION
104 APPLICATION PARTITION DEVICE ASSISTED SERVICE AGENTS
106A APP
106B APP
106C APP
108 OS NETWORKING STACK AND/OR KERNAL PARTITION DEVICE ASSISTED SERVICE AGENTS
116 BUS DRIVER
112 KERNEL EXECUTION PARTITION
114 PROTECTED DEVICE ASSISTED SERVICE EXECUTION PARTITION
110 PROTECTED DAS PARTITION DEVICE ASSISTED SERVICE AGENTS
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
124 MODEM EXECUTION PARTITION
126 MODEM PARTITION DEVICE ASSISTED SERVICE AGENTS
128 MODEM
130 MODEM SERVICE CONTROL LINK
132 MODEM SECURE CHANNEL # N
134 MODEM SECURE CHANNEL # 1
125 MODEM SUB SYSTEM # 1
127 MODEM SUB SYSTEM # N
142 ACCESS NETWORK SVC USAGE
144 PRIVATE NETWORK SVC USAGE
148 BILLING, MEDIATION, SERVICE USAGE LOG, RECONCILATION
136 ACCESS NETWORK # 1
138 ACCESS NETWORK # N
140 INTERNET
146 PRIVATE NETWORK
1442

FIG. 1

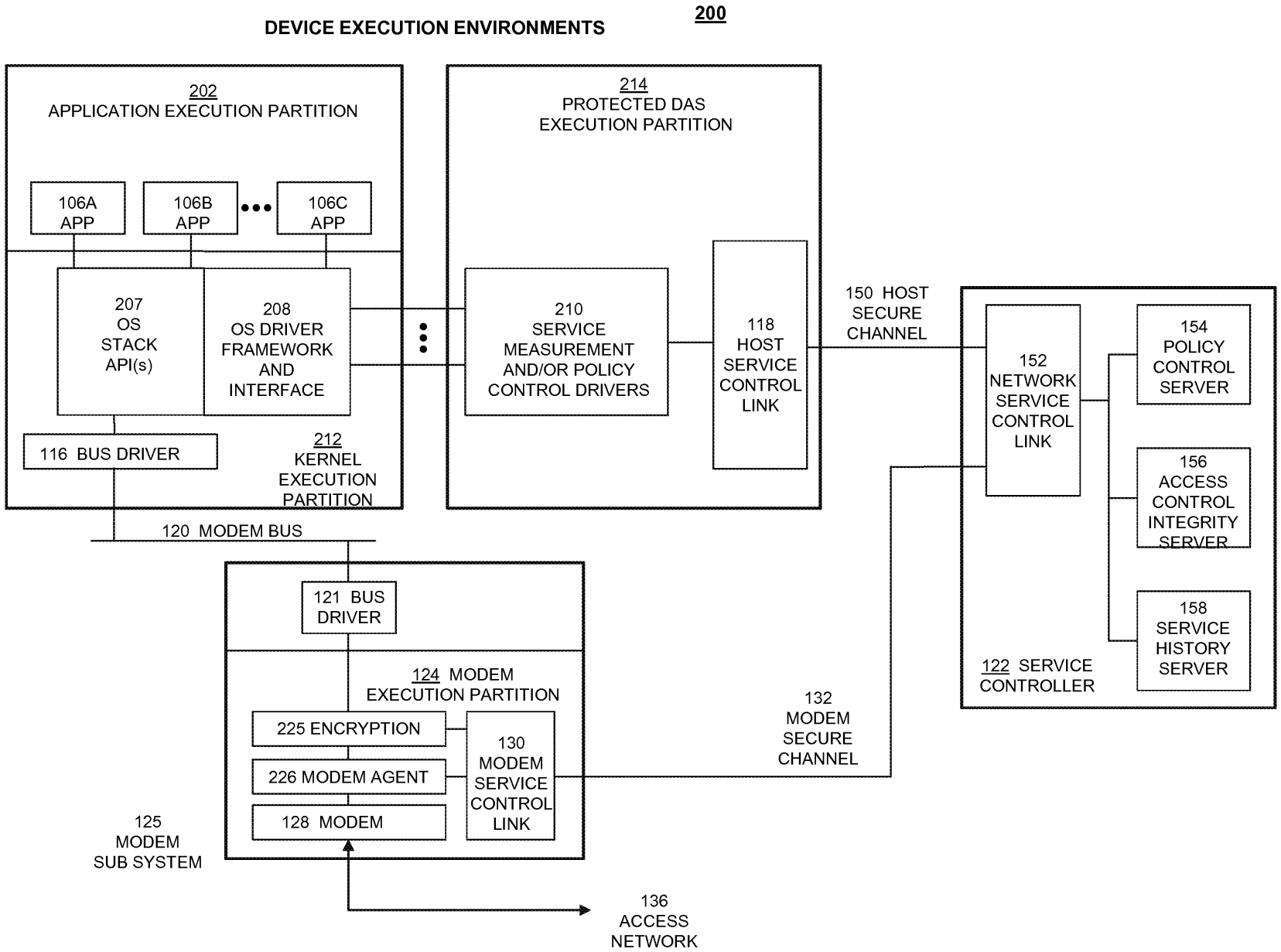

DEVICE EXECUTION ENVIRONMENTS
200
202
APPLICATION EXECUTION PARTITION
106A APP
106B APP
106C APP
207 OS STACK API(s)
208 OS DRIVER FRAMEWORK AND INTERFACE
116 BUS DRIVER
212 KERNEL EXECUTION PARTITION
214
PROTECTED DAS EXECUTION PARTITION
210 SERVICE MEASUREMENT AND/OR POLICY CONTROL DRIVERS
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
124 MODEM EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130 MODEM SERVICE CONTROL LINK
132 MODEM SECURE CHANNEL
125 MODEM SUB SYSTEM
136 ACCESS NETWORK

FIG. 2

1443

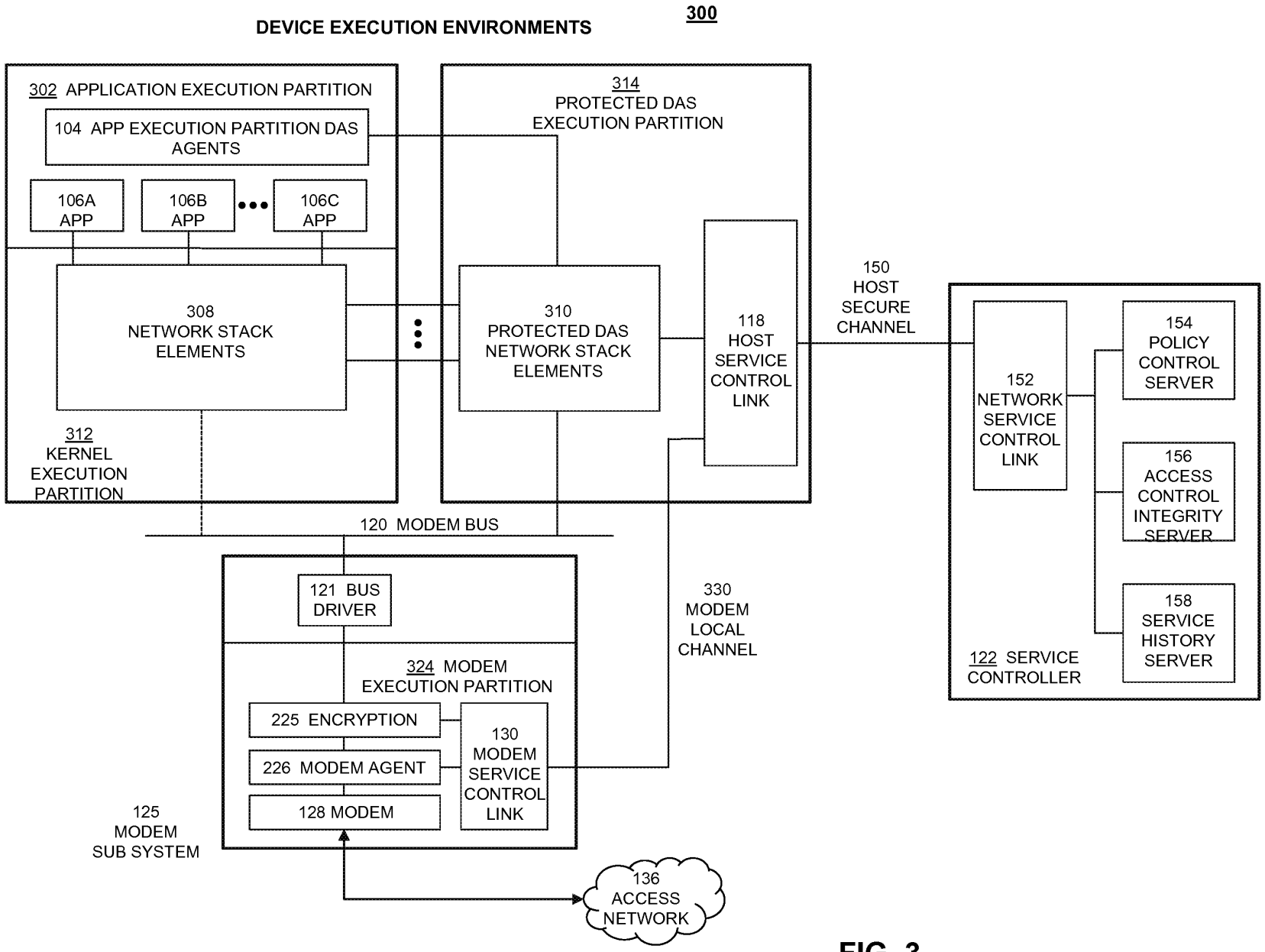

DEVICE EXECUTION ENVIRONMENTS
300
302 APPLICATION EXECUTION PARTITION
104 APP EXECUTION PARTITION DAS AGENTS
106A APP
106B APP
106C APP
308 NETWORK STACK ELEMENTS
312 KERNEL EXECUTION PARTITION
314 PROTECTED DAS EXECUTION PARTITION
310 PROTECTED DAS NETWORK STACK ELEMENTS
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
330 MODEM LOCAL CHANNEL
324 MODEM EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130 MODEM SERVICE CONTROL LINK
125 MODEM SUB SYSTEM
136 ACCESS NETWORK
1444

FIG. 3

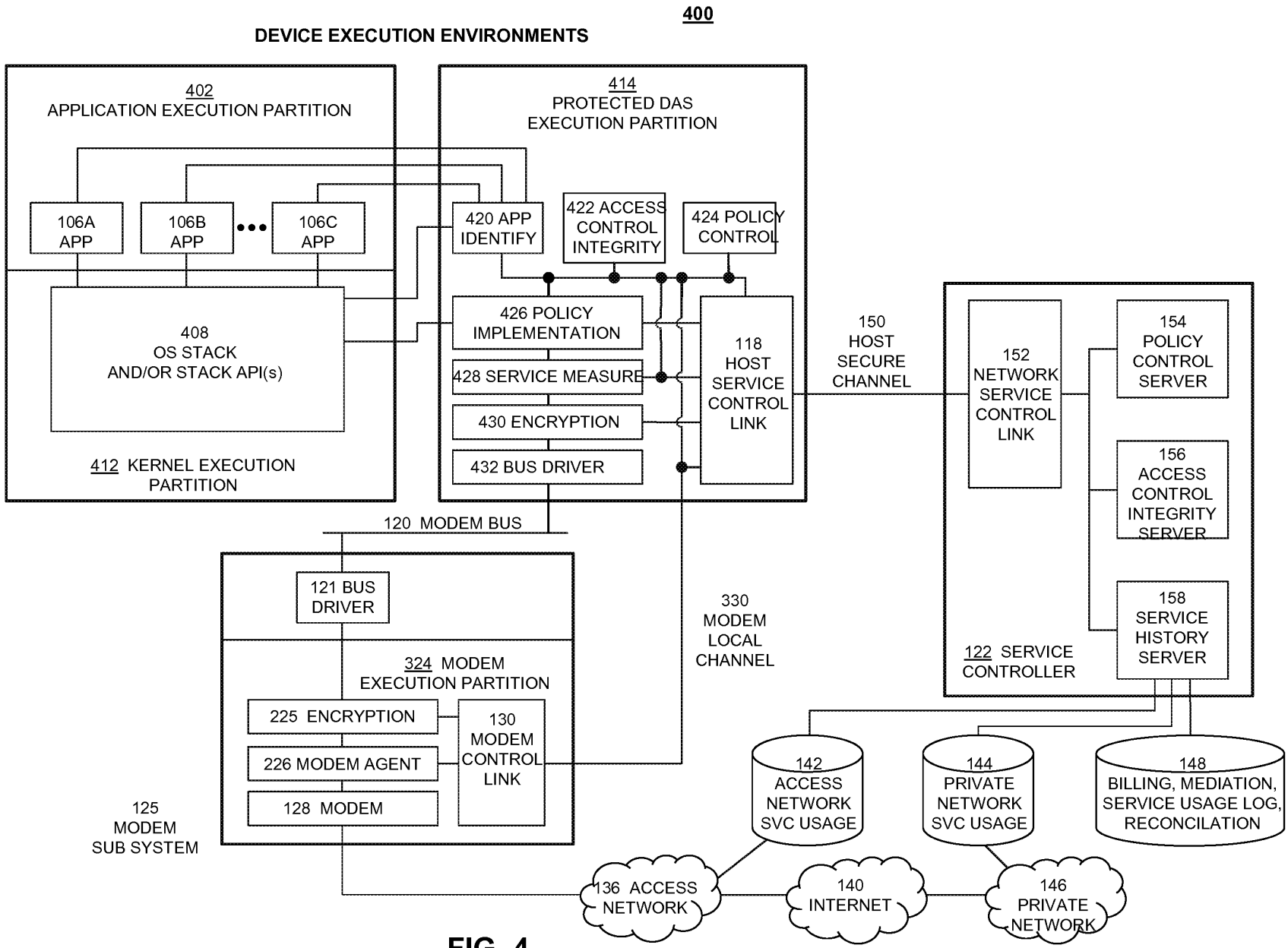

400
DEVICE EXECUTION ENVIRONMENTS
402
APPLICATION EXECUTION PARTITION
106A APP
106B APP
106C APP
408 OS STACK AND/OR STACK API(s)
412 KERNEL EXECUTION PARTITION
414
PROTECTED DAS EXECUTION PARTITION
420 APP IDENTIFY
422 ACCESS CONTROL INTEGRITY
424 POLICY CONTROL
426 POLICY IMPLEMENTATION
428 SERVICE MEASURE
430 ENCRYPTION
432 BUS DRIVER
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
330 MODEM LOCAL CHANNEL
324 MODEM EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130 MODEM CONTROL LINK
125 MODEM SUB SYSTEM
142 ACCESS NETWORK SVC USAGE
144 PRIVATE NETWORK SVC USAGE
148 BILLING, MEDIATION, SERVICE USAGE LOG, RECONCILATION
136 ACCESS NETWORK
140 INTERNET
146 PRIVATE NETWORK
1445

FIG. 4

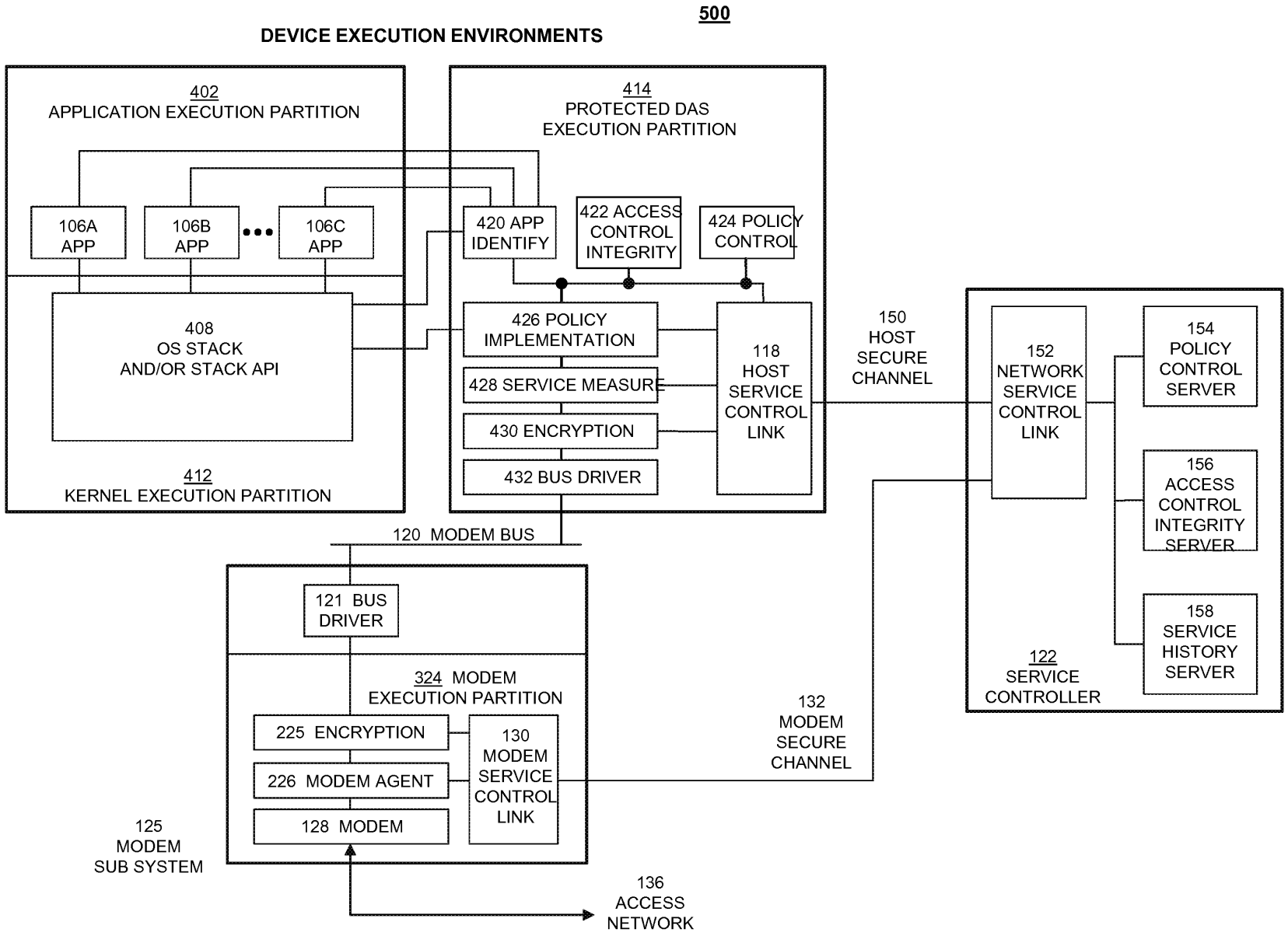

500
DEVICE EXECUTION ENVIRONMENTS
402
APPLICATION EXECUTION PARTITION
106A APP
106B APP
106C APP
408 OS STACK AND/OR STACK API
412
KERNEL EXECUTION PARTITION
414
PROTECTED DAS EXECUTION PARTITION
420 APP IDENTIFY
422 ACCESS CONTROL INTEGRITY
424 POLICY CONTROL
426 POLICY IMPLEMENTATION
428 SERVICE MEASURE
430 ENCRYPTION
432 BUS DRIVER
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
324 MODEM EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130 MODEM SERVICE CONTROL LINK
132 MODEM SECURE CHANNEL
125 MODEM SUB SYSTEM
136 ACCESS NETWORK
1446

FIG. 5

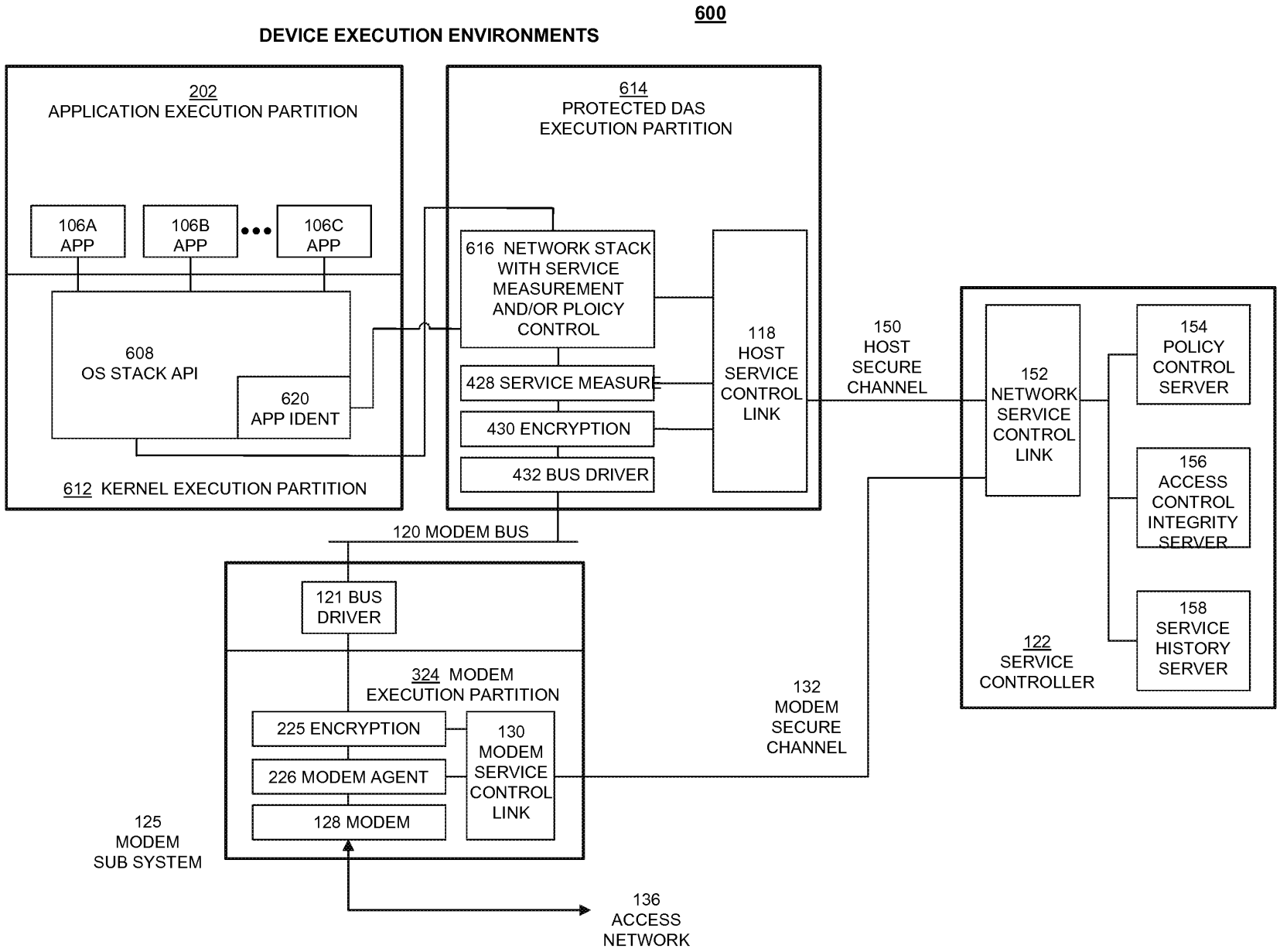

600
DEVICE EXECUTION ENVIRONMENTS
202
APPLICATION EXECUTION PARTITION
106A APP
106B APP
106C APP
608
OS STACK API
620
APP IDENT
612 KERNEL EXECUTION PARTITION
614
PROTECTED DAS
EXECUTION PARTITION
616 NETWORK STACK WITH SERVICE MEASUREMENT AND/OR PLOICY CONTROL
428 SERVICE MEASURE
430 ENCRYPTION
432 BUS DRIVER
118
HOST
SERVICE
CONTROL
LINK
150
HOST
SECURE
CHANNEL
152
NETWORK
SERVICE
CONTROL
LINK
154
POLICY
CONTROL
SERVER
156
ACCESS
CONTROL
INTEGRITY
SERVER
158
SERVICE
HISTORY
SERVER
122
SERVICE
CONTROLLER
120 MODEM BUS
121 BUS
DRIVER
324 MODEM
EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130
MODEM
SERVICE
CONTROL
LINK
132
MODEM
SECURE
CHANNEL
125
MODEM
SUB SYSTEM
136
ACCESS
NETWORK

FIG. 6

1447

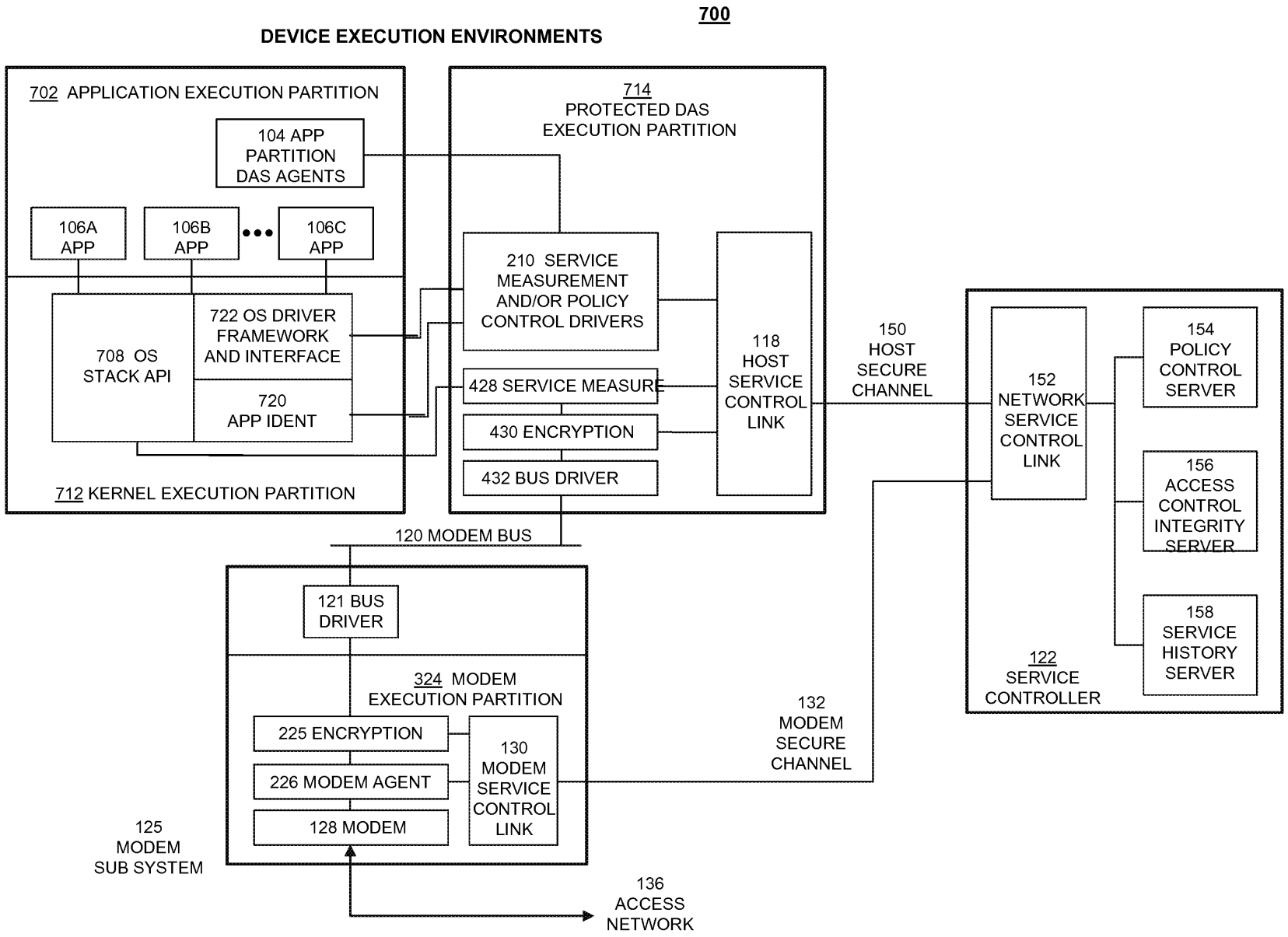

700
DEVICE EXECUTION ENVIRONMENTS
702 APPLICATION EXECUTION PARTITION
104 APP PARTITION DAS AGENTS
106A APP
106B APP
106C APP
708 OS STACK API
722 OS DRIVER FRAMEWORK AND INTERFACE
720 APP IDENT
712 KERNEL EXECUTION PARTITION
714 PROTECTED DAS EXECUTION PARTITION
210 SERVICE MEASUREMENT AND/OR POLICY CONTROL DRIVERS
428 SERVICE MEASURE
430 ENCRYPTION
432 BUS DRIVER
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
324 MODEM EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130 MODEM SERVICE CONTROL LINK
132 MODEM SECURE CHANNEL
125 MODEM SUB SYSTEM
136 ACCESS NETWORK
1448

FIG. 7

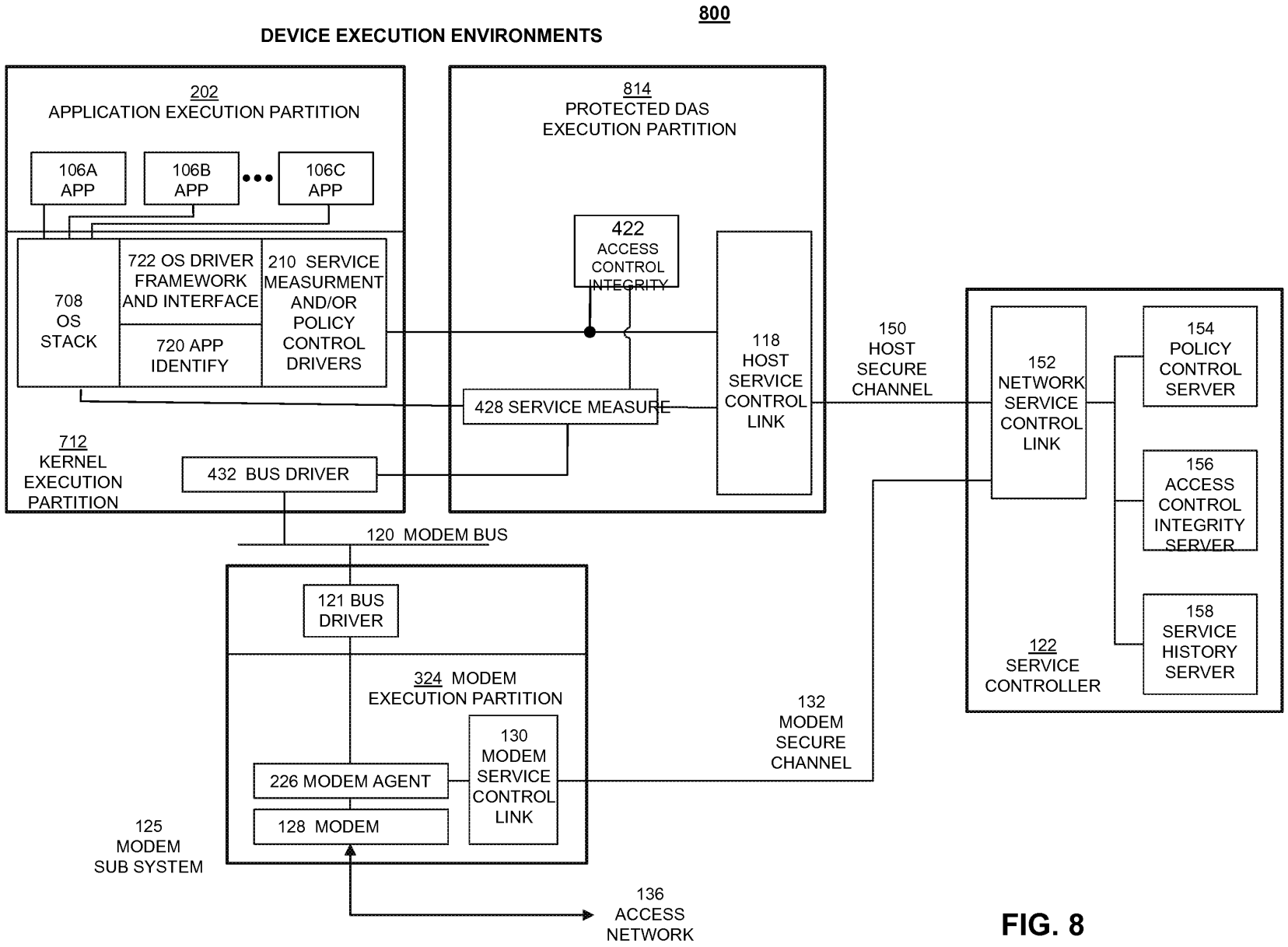

800
DEVICE EXECUTION ENVIRONMENTS
202
APPLICATION EXECUTION PARTITION
106A APP
106B APP
106C APP
708 OS STACK
722 OS DRIVER FRAMEWORK AND INTERFACE
720 APP IDENTIFY
210 SERVICE MEASURMENT AND/OR POLICY CONTROL DRIVERS
712 KERNEL EXECUTION PARTITION
432 BUS DRIVER
814
PROTECTED DAS EXECUTION PARTITION
422 ACCESS CONTROL INTEGRITY
428 SERVICE MEASURE
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
324 MODEM EXECUTION PARTITION
130 MODEM SERVICE CONTROL LINK
132 MODEM SECURE CHANNEL
226 MODEM AGENT
128 MODEM
125 MODEM SUB SYSTEM
136 ACCESS NETWORK

FIG. 8

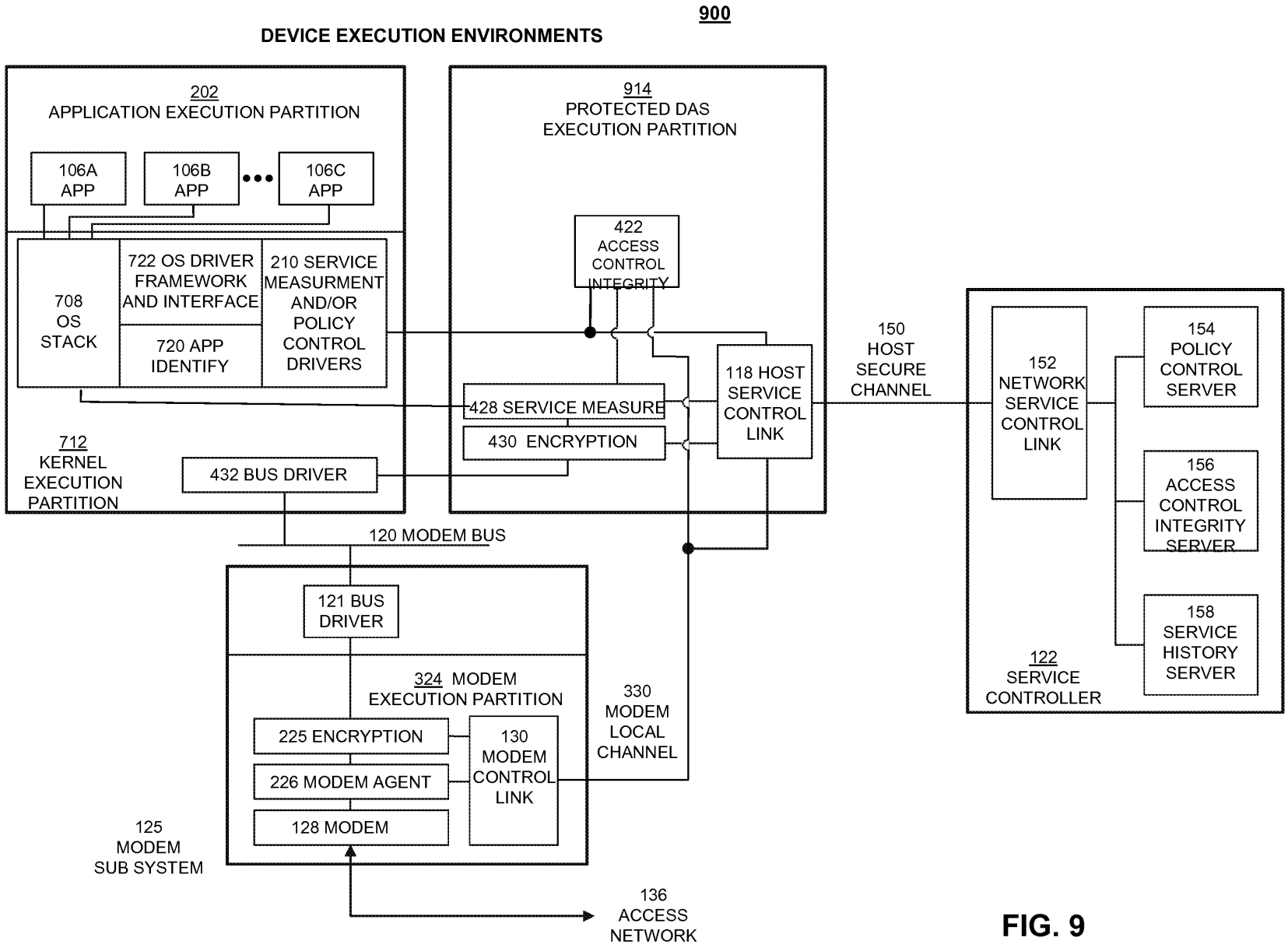

900
DEVICE EXECUTION ENVIRONMENTS
202
APPLICATION EXECUTION PARTITION
106A APP
106B APP
106C APP
708 OS STACK
722 OS DRIVER FRAMEWORK AND INTERFACE
720 APP IDENTIFY
210 SERVICE MEASURMENT AND/OR POLICY CONTROL DRIVERS
712 KERNEL EXECUTION PARTITION
432 BUS DRIVER
914 PROTECTED DAS EXECUTION PARTITION
422 ACCESS CONTROL INTEGRITY
428 SERVICE MEASURE
430 ENCRYPTION
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
324 MODEM EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130 MODEM CONTROL LINK
330 MODEM LOCAL CHANNEL
125 MODEM SUB SYSTEM
136 ACCESS NETWORK
1450

FIG. 9

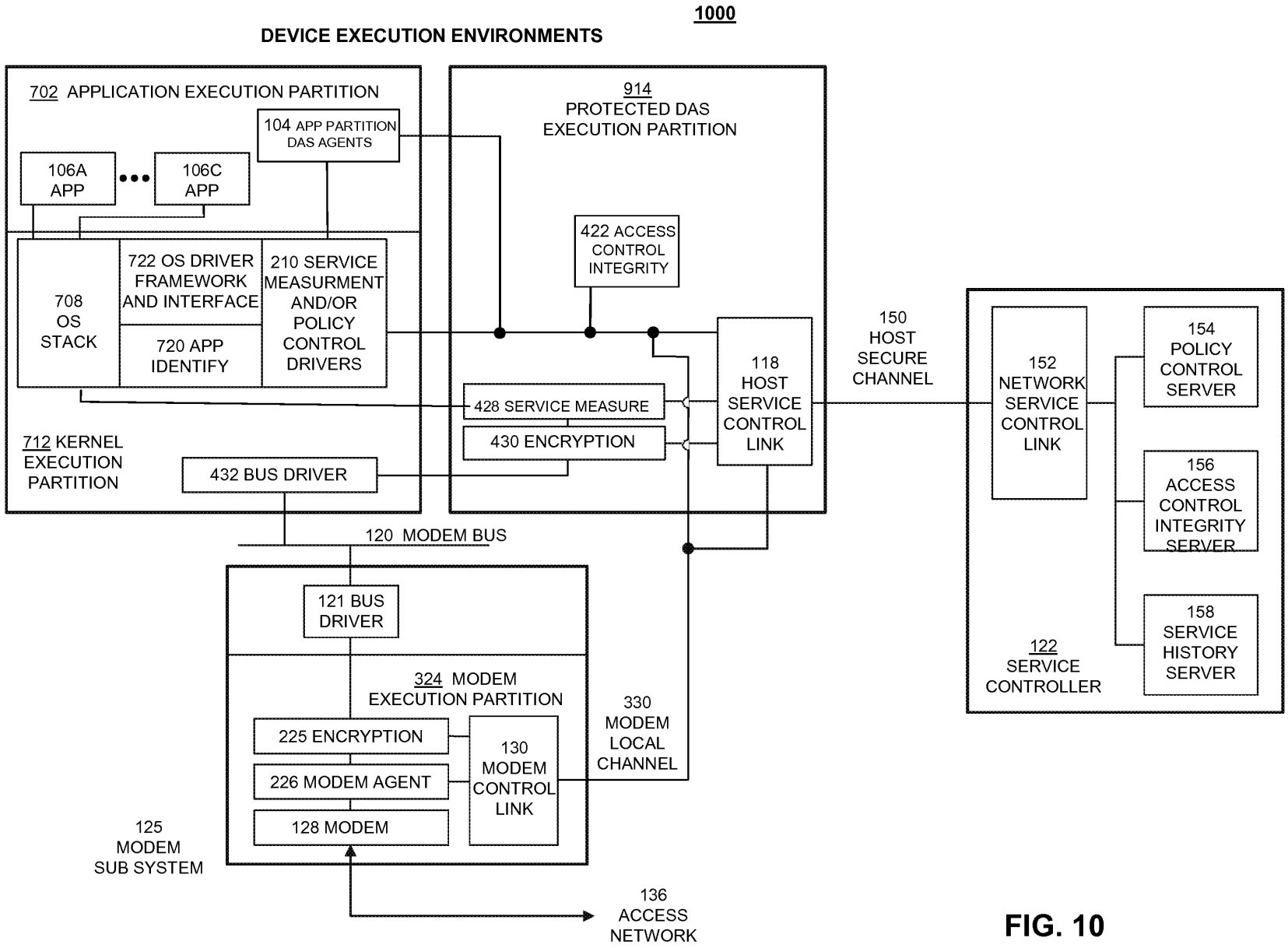

1000
DEVICE EXECUTION ENVIRONMENTS
1451
702 APPLICATION EXECUTION PARTITION
104 APP PARTITION DAS AGENTS
106A APP
106C APP
708 OS STACK
722 OS DRIVER FRAMEWORK AND INTERFACE
720 APP IDENTIFY
210 SERVICE MEASURMENT AND/OR POLICY CONTROL DRIVERS
712 KERNEL EXECUTION PARTITION
432 BUS DRIVER
914 PROTECTED DAS EXECUTION PARTITION
422 ACCESS CONTROL INTEGRITY
428 SERVICE MEASURE
430 ENCRYPTION
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
120 MODEM BUS
121 BUS DRIVER
324 MODEM EXECUTION PARTITION
225 ENCRYPTION
226 MODEM AGENT
128 MODEM
130 MODEM CONTROL LINK
330 MODEM LOCAL CHANNEL
125 MODEM SUB SYSTEM
136 ACCESS NETWORK

FIG. 10

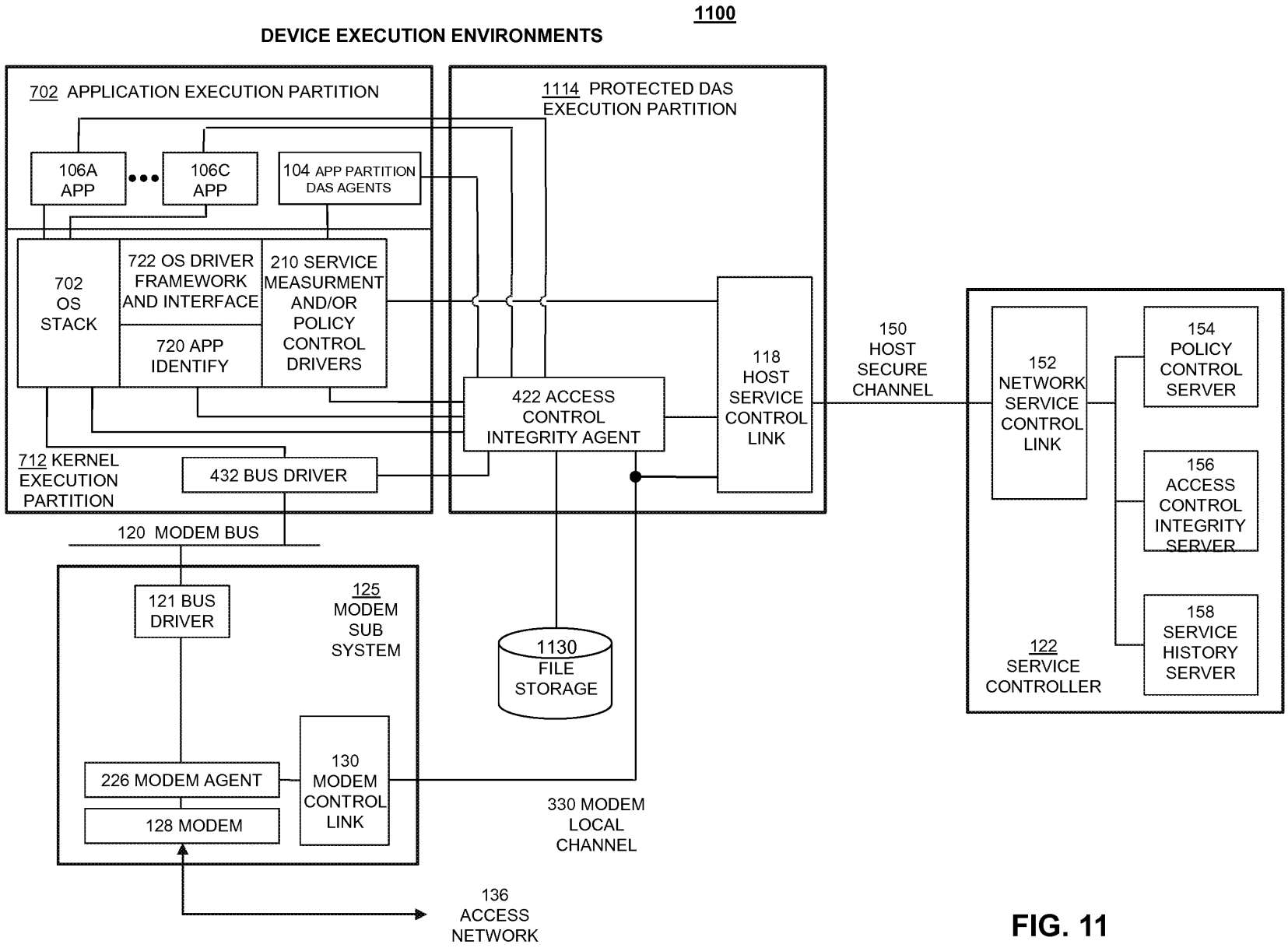

1100
DEVICE EXECUTION ENVIRONMENTS
702 APPLICATION EXECUTION PARTITION
1114 PROTECTED DAS EXECUTION PARTITION
106A APP
106C APP
104 APP PARTITION DAS AGENTS
702 OS STACK
722 OS DRIVER FRAMEWORK AND INTERFACE
720 APP IDENTIFY
210 SERVICE MEASURMENT AND/OR POLICY CONTROL DRIVERS
422 ACCESS CONTROL INTEGRITY AGENT
118 HOST SERVICE CONTROL LINK
150 HOST SECURE CHANNEL
152 NETWORK SERVICE CONTROL LINK
154 POLICY CONTROL SERVER
156 ACCESS CONTROL INTEGRITY SERVER
158 SERVICE HISTORY SERVER
122 SERVICE CONTROLLER
712 KERNEL EXECUTION PARTITION
432 BUS DRIVER
120 MODEM BUS
121 BUS DRIVER
125 MODEM SUB SYSTEM
1130 FILE STORAGE
226 MODEM AGENT
128 MODEM
130 MODEM CONTROL LINK
330 MODEM LOCAL CHANNEL
136 ACCESS NETWORK
1452

FIG. 11

# Electronic Acknowledgement Receipt

| | |
|---|---|
| **EFS ID:** | 6885018 |
| **Application Number:** | 12694445 |
| **International Application Number:** | |
| **Confirmation Number:** | 6030 |
| **Title of Invention:** | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES |
| **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:** | RALEP025 |
| **Receipt Date:** | 27-JAN-2010 |
| **Filing Date:** | |
| **Time Stamp:** | 12:51:55 |
| **Application Type:** | Utility under 35 USC 111(a) |

## Payment information:

| | |
|---|---|
| Submitted with Payment | no |

## File Listing:

| Document Number | Document Description | File Name | File Size(Bytes)/ Message Digest | Multi Part /.zip | Pages (if appl.) |
|---|---|---|---|---|---|
| 1 | Application Data Sheet | RALEP025_Application_Data_Sheet_sb0014_fill.pdf | 964990<br>b892691f2fd675755899b53d8838ab0b985dc685 | no | 5 |

| | |
|---|---|
| **Warnings:** | |
| **Information:** | |

| | | | | | |
|---|---|---|---|---|---|
| 2 | | RALEP025_APP.pdf | 174625<br>675f05d52a6353a2d558c4e291181ae544c5d6cc | yes | 38 |

| | Multipart Description/PDF files in .zip description | | |
|---|---|---|---|
| | **Document Description** | **Start** | **End** |
| | Transmittal of New Application | 1 | 1 |
| | Specification | 2 | 30 |
| | Claims | 31 | 37 |
| | Abstract | 38 | 38 |

**Warnings:**

**Information:**

| | | | | | |
|---|---|---|---|---|---|
| 3 | Drawings-only black and white line drawings | RALEP025_Figures.pdf | 152514<br>40617466ffbee7c3aac6657d1986588d25aa98c7 | no | 11 |

**Warnings:**

**Information:**

| | |
|---|---|
| **Total Files Size (in bytes):** | 1292129 |

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

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

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

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

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | RALEP025 |
|---|---|---|
| | Application Number | |
| Title of Invention | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | |

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

## Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

## Applicant Information:

**Applicant 1** Remove

**Applicant Authority** ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

| Prefix | Given Name | Middle Name | Family Name | Suffix |
|---|---|---|---|---|
| | Gregory | G. | Raleigh | |

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

| City | Woodside | State/Province | CA | Country of Residence [i] | US |
|---|---|---|---|---|---|

**Citizenship under 37 CFR 1.41(b)** [i] US

**Mailing Address of Applicant:**

| Address 1 | 2995 Woodside Road |
|---|---|
| Address 2 | Suite 400 |

| City | Woodside | State/Province | CA |
|---|---|---|---|
| Postal Code | 94062 | Country [i] | |

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

## Correspondence Information:

**Enter either Customer Number or complete the Correspondence Information section below.**
**For further information see 37 CFR 1.33(a).**

☐ **An Address is being provided for the correspondence Information of this application.**

| Customer Number | 21912 | | |
|---|---|---|---|
| Email Address | | Add Email | Remove Email |

## Application Information:

| Title of the Invention | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | | |
|---|---|---|---|
| Attorney Docket Number | RALEP025 | Small Entity Status Claimed | ☐ |
| Application Type | Nonprovisional | | |
| Subject Matter | Utility | | |
| Suggested Class (if any) | | Sub Class (if any) | |
| Suggested Technology Center (if any) | | | |
| Total Number of Drawing Sheets (if any) | 11 | Suggested Figure for Publication (if any) | |

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| Application Data Sheet 37 CFR 1.76 | Attorney Docket Number | RALEP025 |
|---|---|---|
| | Application Number | |
| Title of Invention | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | |

## Publication Information:

| |
|---|
| ☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219) |
| ☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing. |

## Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

| Please Select One: | ◉ Customer Number | ○ US Patent Practitioner | ○ Limited Recognition (37 CFR 11.9) |
|---|---|---|---|
| Customer Number | 21912 | | |

## Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

| Prior Application Status | Pending | | Remove |
|---|---|---|---|
| Application Number | Continuity Type | Prior Application Number | Filing Date (YYYY-MM-DD) |
| | Continuation in part of | 12380780 | 2009-03-02 |
| Prior Application Status | Pending | | Remove |
| Application Number | Continuity Type | Prior Application Number | Filing Date (YYYY-MM-DD) |
| | non provisional of | 61206354 | 2009-01-28 |
| Prior Application Status | Pending | | Remove |
| Application Number | Continuity Type | Prior Application Number | Filing Date (YYYY-MM-DD) |
| | non provisional of | 61206944 | 2009-02-04 |
| Prior Application Status | Pending | | Remove |
| Application Number | Continuity Type | Prior Application Number | Filing Date (YYYY-MM-DD) |
| | non provisional of | 61207393 | 2009-02-10 |
| Prior Application Status | | | Remove |
| Application Number | Continuity Type | Prior Application Number | Filing Date (YYYY-MM-DD) |
| | non provisional of | 61207739 | 2009-02-13 |
| Prior Application Status | | | Remove |

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| **Application Data Sheet 37 CFR 1.76** | Attorney Docket Number | RALEP025 |
|---|---|---|
| | Application Number | |
| Title of Invention | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | |

| Application Number | Continuity Type | Prior Application Number | Filing Date (YYYY-MM-DD) |
|---|---|---|---|
| | non provisional of | 61252151 | 2009-10-15 |

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

## Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

| Application Number | Country [i] | Parent Filing Date (YYYY-MM-DD) | Priority Claimed |
|---|---|---|---|
| | | | ◉ Yes ○ No |

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

## Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

**Assignee 1** Remove

If the Assignee is an Organization check here. ☒

| Organization Name | Headwater Partners I LLC | | |
|---|---|---|---|
| **Mailing Address Information:** | | | |
| **Address 1** | 2995 Woodside Road | | |
| Address 2 | Suite 400 | | |
| **City** | Woodside | **State/Province** | CA |
| **Country** [i] US | | Postal Code | 94062 |
| Phone Number | | Fax Number | |
| Email Address | | | |

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

## Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

| **Signature** | /Michael J. Schallop/ | | | Date (YYYY-MM-DD) | 2010-01-27 |
|---|---|---|---|---|---|
| First Name | Michael | Last Name | Schallop | Registration Number | 44319 |

PTO/SB/14 (07-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

| **Application Data Sheet 37 CFR 1.76** | Attorney Docket Number | RALEP025 |
|---|---|---|
| | Application Number | |
| Title of Invention | SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES | |

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

# Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/06 (12-04)

**Date:** **01/27/10**

Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

**PATENT APPLICATION FEE DETERMINATION RECORD**
Substitute for Form PTO-875

Application or Docket Number
12/694,445

## APPLICATION AS FILED – PART I

| FOR | (Column 1) NUMBER FILED | (Column 2) NUMBER EXTRA | SMALL ENTITY RATE ($) | SMALL ENTITY FEE ($) | OR | OTHER THAN SMALL ENTITY RATE ($) | OTHER THAN SMALL ENTITY FEE ($) |
|---|---|---|---|---|---|---|---|
| BASIC FEE (37 CFR 1.16(a), (b), or (c)) | N/A | N/A | N/A | | | N/A | 330 |
| SEARCH FEE (37 CFR 1.16(k), (i), or (m)) | N/A | N/A | N/A | | | N/A | 540 |
| EXAMINATION FEE (37 CFR 1.16(o), (p), or (q)) | N/A | N/A | N/A | | | N/A | 220 |
| TOTAL CLAIMS (37 CFR 1.16(i)) | 25 minus 20 = | 5 | x$26 | | OR | x$52 | 260 |
| INDEPENDENT CLAIMS (37 CFR 1.16(h)) | 3 minus 3 = | * | x$110 | | | x$220 | |
| APPLICATION SIZE FEE (37 CFR 1.16(s)) | If the specification and drawings exceed 100 sheets of paper, the application size fee due is $260 ($130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR | | | | | | |
| MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j)) | | | 195 | | | 390 | |
| | | | TOTAL | | | TOTAL | 1350 |

* If the difference in column 1 is less than zero, enter "0" in column 2.

## APPLICATION AS AMENDED – PART II

| | | (Column 1) CLAIMS REMAINING AFTER AMENDMENT | | (Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR | (Column 3) PRESENT EXTRA | SMALL ENTITY RATE ($) | SMALL ENTITY ADDITIONAL FEE ($) | OR | OTHER THAN SMALL ENTITY RATE ($) | OTHER THAN SMALL ENTITY ADDITIONAL FEE ($) |
|---|---|---|---|---|---|---|---|---|---|---|
| AMENDMENT A | Total (37 CFR 1.16(i)) | * | Minus | ** | = | x = | | OR | x = | |
| | Independent (37 CFR 1.16(h)) | * | Minus | *** | = | x = | | OR | x = | |
| | Application Size Fee (37 CFR 1.16(s)) | | | | | | | | | |
| | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j)) | | | | | N/A | | OR | N/A | |
| | | | | | | TOTAL ADD'T FEE | | OR | TOTAL ADD'T FEE | |

| | | (Column 1) CLAIMS REMAINING AFTER AMENDMENT | | (Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR | (Column 3) PRESENT EXTRA | RATE ($) | ADDITIONAL FEE ($) | OR | RATE ($) | ADDITIONAL FEE ($) |
|---|---|---|---|---|---|---|---|---|---|---|
| AMENDMENT B | Total (37 CFR 1.16(i)) | * | Minus | ** | = | x = | | OR | x = | |
| | Independent (37 CFR 1.16(h)) | * | Minus | *** | = | x = | | OR | x = | |
| | Application Size Fee (37 CFR 1.16(s)) | | | | | | | | | |
| | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j)) | | | | | N/A | | OR | N/A | |
| | | | | | | TOTAL ADD'T FEE | | OR | TOTAL ADD'T FEE | |

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*