

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.

10 [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
5 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
10 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
15 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
20 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
25 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).

30 [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.

5 [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
10 202 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
15 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
20 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.

25 [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
30 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.

5 [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)
10 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.

15 [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
20 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
25 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
30 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.

- 5 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
10 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
15 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
20 214 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
25 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,
30 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.

5 [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, 10 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 15 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 20 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.

25 [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 30 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.

5 [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
10 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
15 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
20 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
25 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,
30 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.

5 [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.

10 [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.

25 [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.

30

WE CLAIM:

- 1 1. A system that manages a plurality of mobile devices associated with a customer,
2 comprising:
3 a customer data store that maintains customer data comprising a customer policy and end
4 user data related to a plurality of end users associated with the customer;
5 a service provider data store that maintains service provider data associated with a
6 plurality of service providers, said service provider data comprising at least one service plan
7 offered by said plurality of service providers;
8 a user interface that provides said plurality of end users and the customer with an
9 interface to the system; and
10 an aggregation component that utilizes said service provider data, said customer policy
11 and said end user data to enable the customer to manage the plurality of mobile devices used by
12 said plurality of end users.
- 1 2. The system of claim 1, further comprising a procurement component that obtains the
2 plurality of mobile devices from said plurality service providers in accordance with said
3 customer policy.
- 1 3. The system of claim 2, wherein said customer policy describes an approval process for
2 procuring a mobile device.
- 1 4. The system of claim 3, wherein said customer policy further describes at least one
2 available service associated with a subset of end users selected from said plurality of end users
3 based, at least in part, upon a characteristic associated with each of said subset of end users.
- 1 5. The system of claim 1, further comprising a billing component that allocates cost
2 associated with the plurality of mobile devices as a function of said customer policy.

1 6. The system of claim 5, whereby said cost from said service providers is partially
2 allocated to the customer for said plurality of end users, with the remainder allocated to said
3 plurality of end users based, at least in part, upon said at least one service plan provisioned for
4 each of said plurality of end users.

1 7. The system of claim 5, said cost is allocated based at least in part upon a customer
2 business unit.

1 8. The system of claim 5, further comprising:
2 an asset data store that maintains asset data corresponding to the plurality of mobile
3 devices; and
4 a reconciliation component that reconciles said cost and usage data associated with the
5 plurality of mobile devices with said customer data, said service provider data and said asset
6 data, said cost and said usage data is obtained from said plurality of service providers.

1 9. The system of claim 8, further comprising a reporting component that generates an
2 exception report detailing exceptions from said customer policy for each of said plurality of end
3 users, based at least in part upon, said cost and said usage data associated with an individual end
4 user selected from said plurality of end users.

1 10. The system of claim 1, wherein said customer data further comprises usage data that
2 describes use characteristics of the plurality of mobile devices by said plurality of end users.

1 11. The system of claim 1, further comprising an optimization component that analyzes said
2 customer data in conjunction with said service provider data and generates a recommendation for
3 reducing cost associated with the plurality of mobile devices.

1 12. The system of claim 1, further comprising a support component adapted to facilitate
2 support for said plurality of end users.

1 13. The system of claim 1, further comprising an asset component that provides the customer
2 with ability to monitor provisioning and use of the plurality of mobile devices to said plurality of
3 end users.

1 14. The system of claim 11, whereby a wireless number for each of the plurality of mobile
2 devices is utilized as a device identifier for monitoring the plurality of mobile devices.

1 15. The system of claim 1, further comprising a means for transforming said customer data
2 into a standardized format for data aggregation and import into an accounting system.

1 16. A method of managing a plurality of mobile devices for a customer, comprising:
2 obtaining customer data indicative of a customer policy, said customer policy related to
3 the plurality of mobile devices;
4 obtaining end user data related to a plurality of end users associated with the customer;
5 obtaining service provider data associated a plurality of service providers;
6 deploying a user interface adapted to facilitate management of the plurality of mobile
7 devices as a function of said customer policy, said service provider data and said end user data;
8 and
9 generating a recommendation to improve management of the plurality of mobile devices
10 in accordance with said customer policy, said end user data and said service provider data.

1 17. The method of claim 16, further comprising procuring at least one of the plurality of
2 mobile devices *via* said user interface.

1 18. The method of claim 17, further comprising authorizing procurement of at least one of
2 the plurality of mobile devices as a function of said customer policy.

1 19. The method of claim 16, further comprising generating an exception report that provides
2 details of usage of at least one of the plurality of mobile devices, said exception report is
3 indicative of a violation of said customer policy.

- 1 20. The method of claim 16, further comprising coordinating support of the plurality of
2 mobile devices from said plurality of service providers for said plurality of end users.
- 1 21. The method of claim 16, further comprising allocating cost for the plurality of mobile
2 devices based at least in part upon a service plan associated with each of the plurality of mobile
3 devices.
- 1 22. The method of claim 16, further comprising allocating cost for the plurality of mobile
2 devices based at least in part upon a characteristic of each of said plurality of end users.
- 1 23. The method of claim 16, further comprising invoicing an individual selected from said
2 plurality of end users for cost associated with a mobile device selected from the plurality of
3 mobile devices, said mobile device is assigned to said individual.
- 1 24. The method of claim 16, further comprising aggregating billing for said plurality of
2 service providers.

1 25. A system for managing a plurality of mobile devices associated with a customer,
2 comprising:
3 a customer data store comprising a customer policy defining procurement and
4 provisioning preferences of the customer, and end user information pertaining to an end user
5 associated with the customer, the end user information comprising an end user characteristic, an
6 end user historical use data, and an end user provisioning history;
7 a service provider data store adapted to store service provider data associated with a
8 plurality of service providers, said service provider data comprising a service plan and a mobile
9 device selected from the plurality of mobile devices associated with said service plan;
10 a user interface adapted to interface with the customer, said user interface includes a
11 means for updating said customer data store and a means for reporting details associated with
12 said service provider data store and said customer data store;
13 means for providing procurement options to said customer, selected by applying said
14 customer policy and said end user information to said service provider data, said procurement
15 options are presented via said user interface;
16 means for procuring said mobile device from one of said plurality of service providers
17 and said service plan from one of said plurality of service providers based at least in part upon
18 input received from the customer via said user interface;
19 means for provisioning said mobile device that activates and provides said service plan
20 and said mobile device to an end user;
21 means for processing an invoice from said plurality of service providers; and
22 means for updating said customer data store with details obtained from said invoice for
23 the customer and updating said end user historical use data with details obtained from said
24 invoice.

1/17

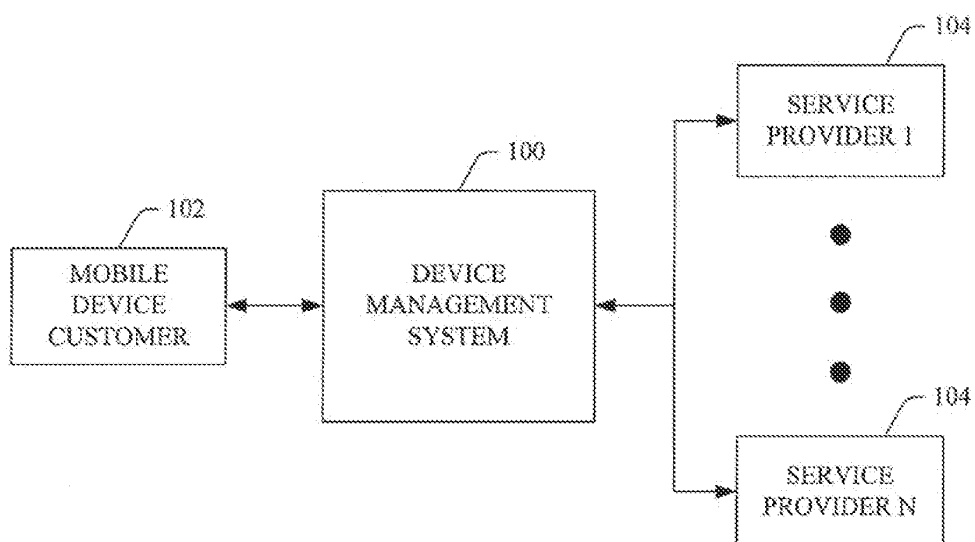


FIG. 1

2/17

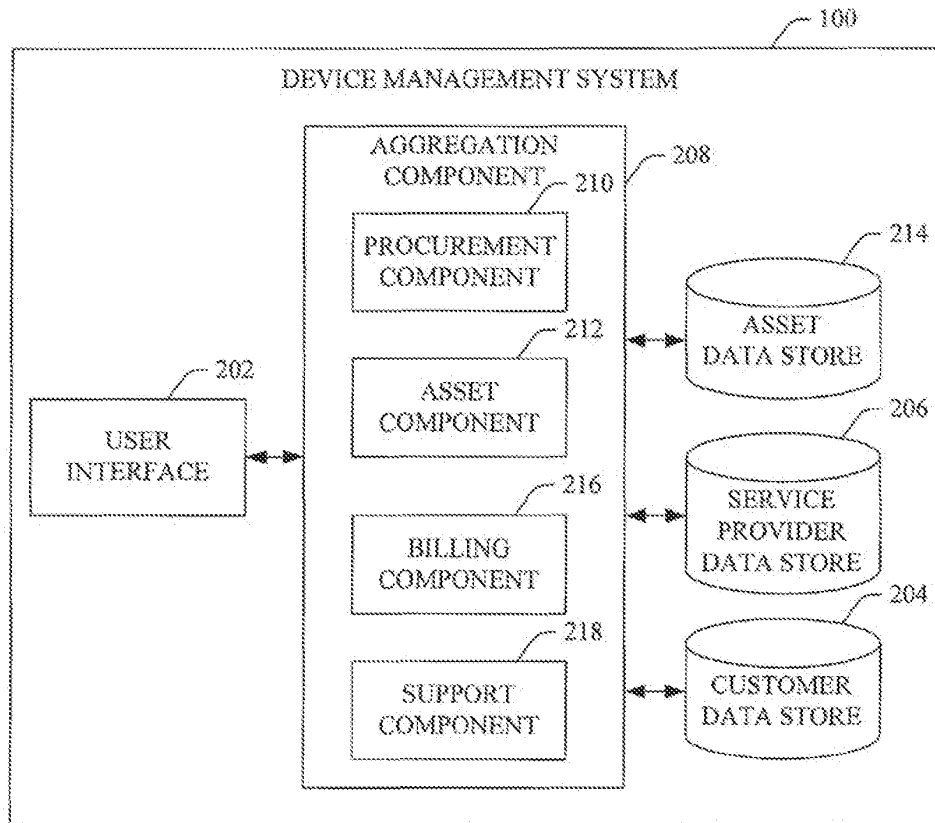


FIG. 2

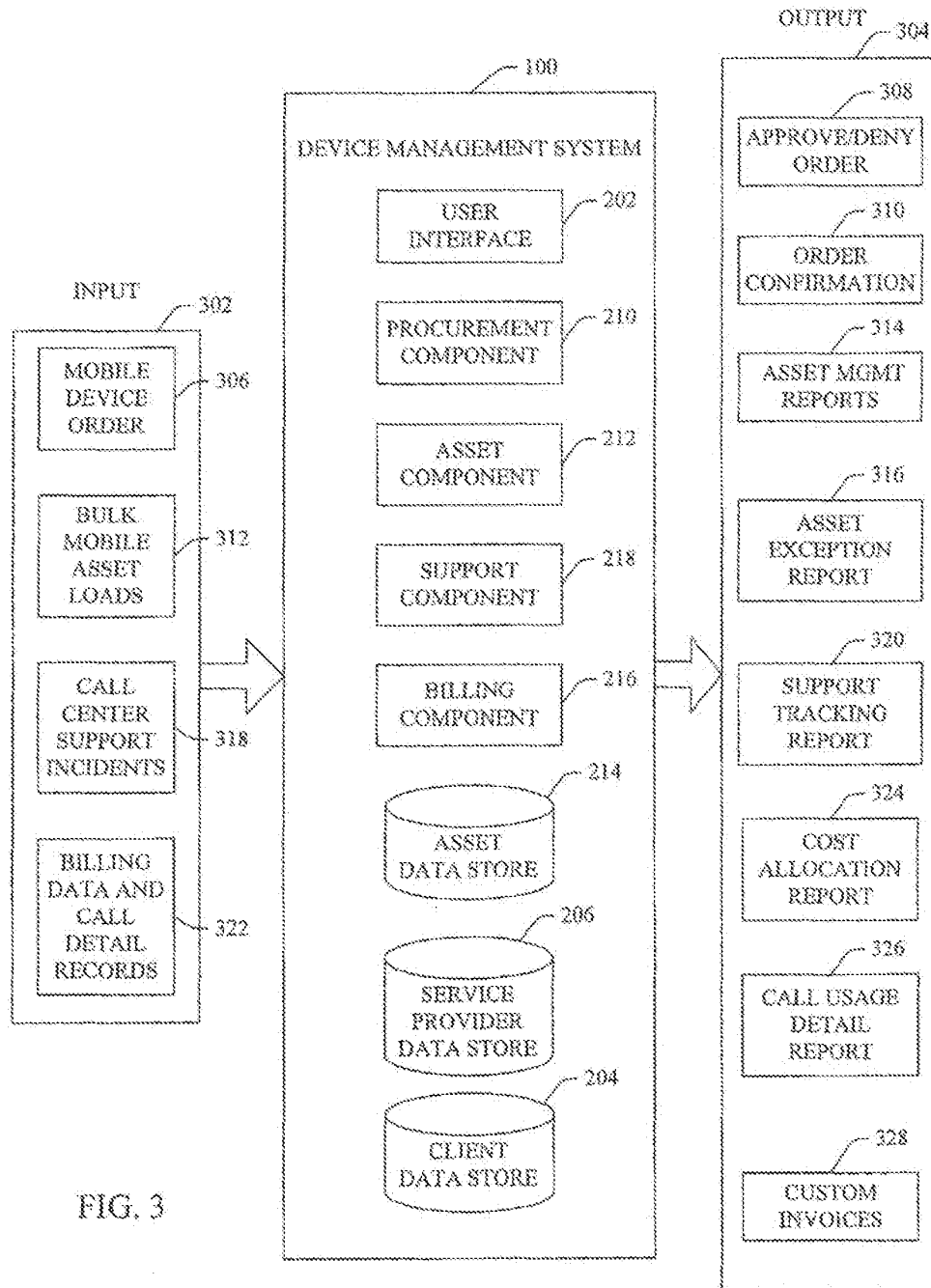


FIG. 3

4/17

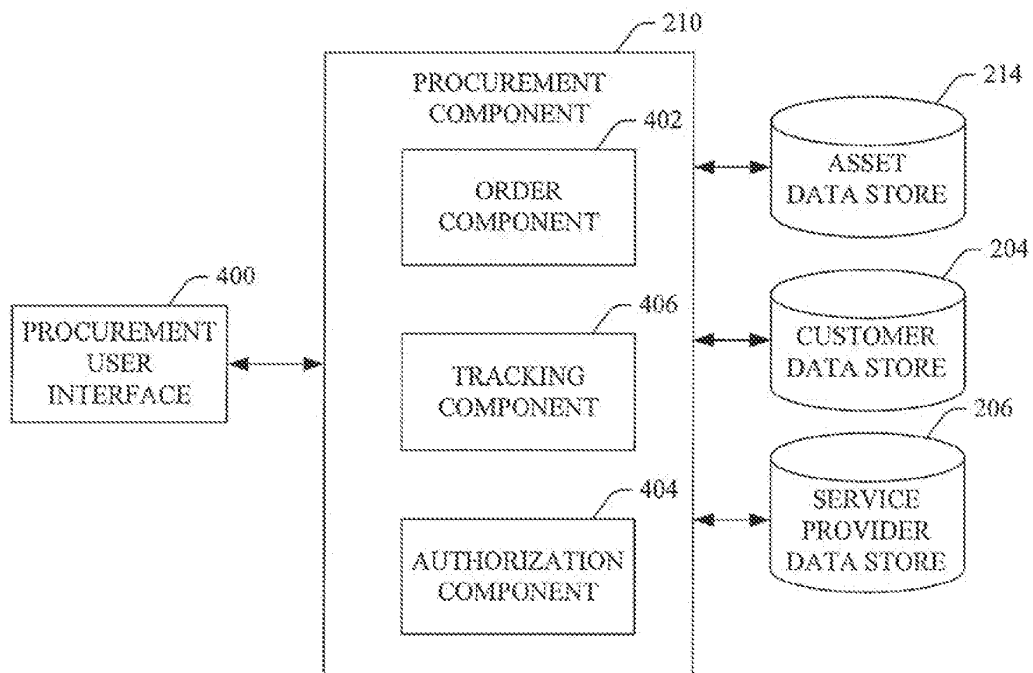


FIG. 4

5/17

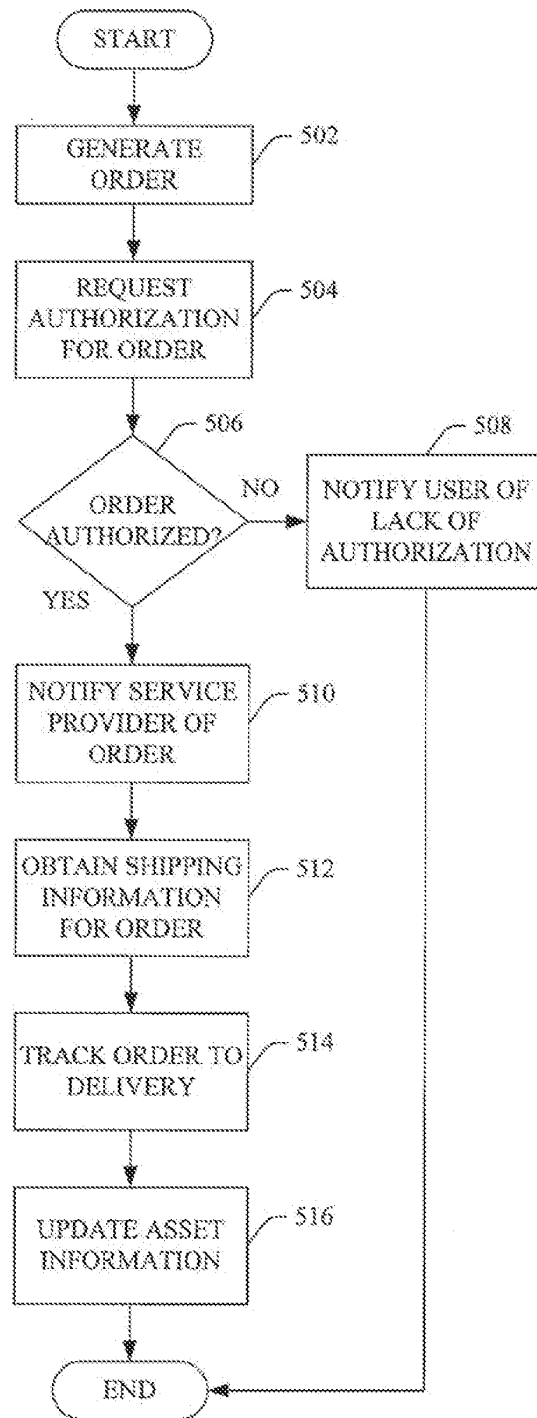


FIG. 5

6/17

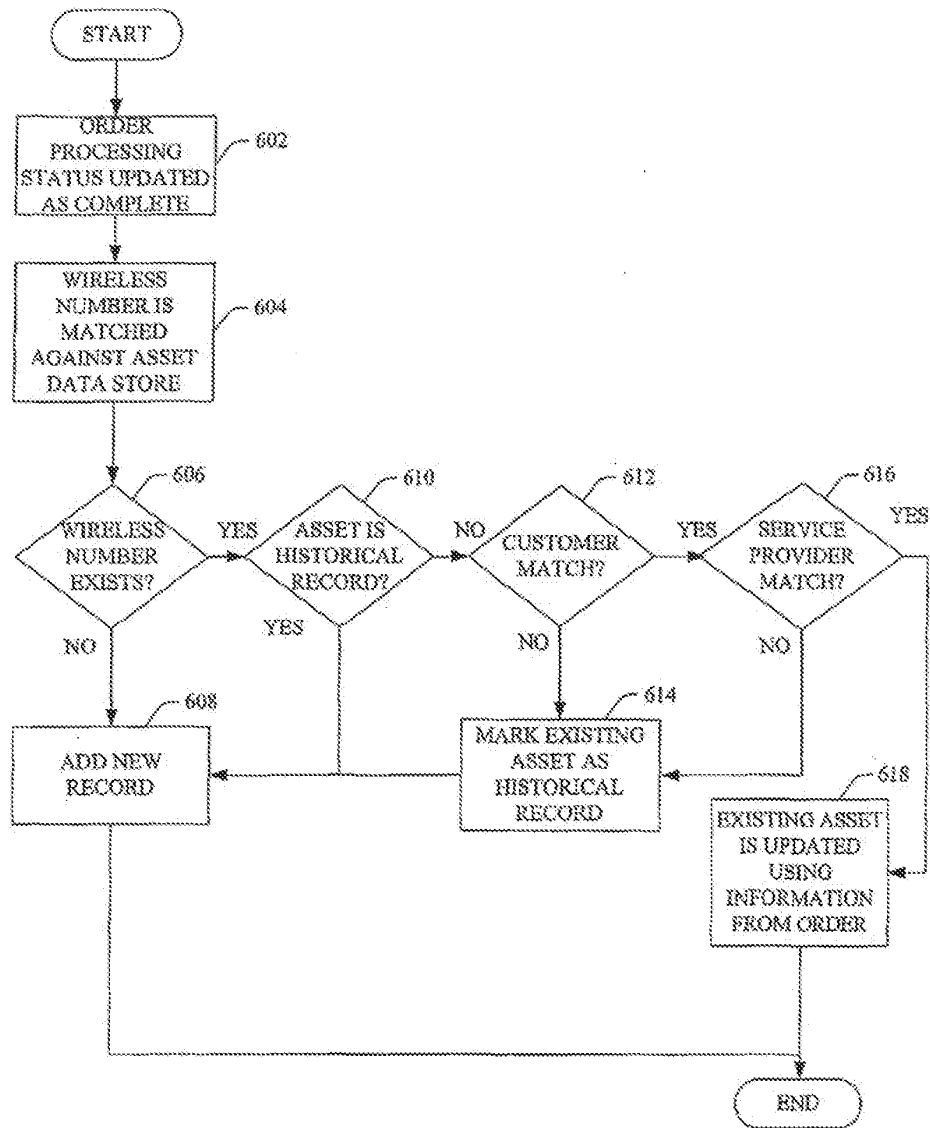


FIG. 6

7/17

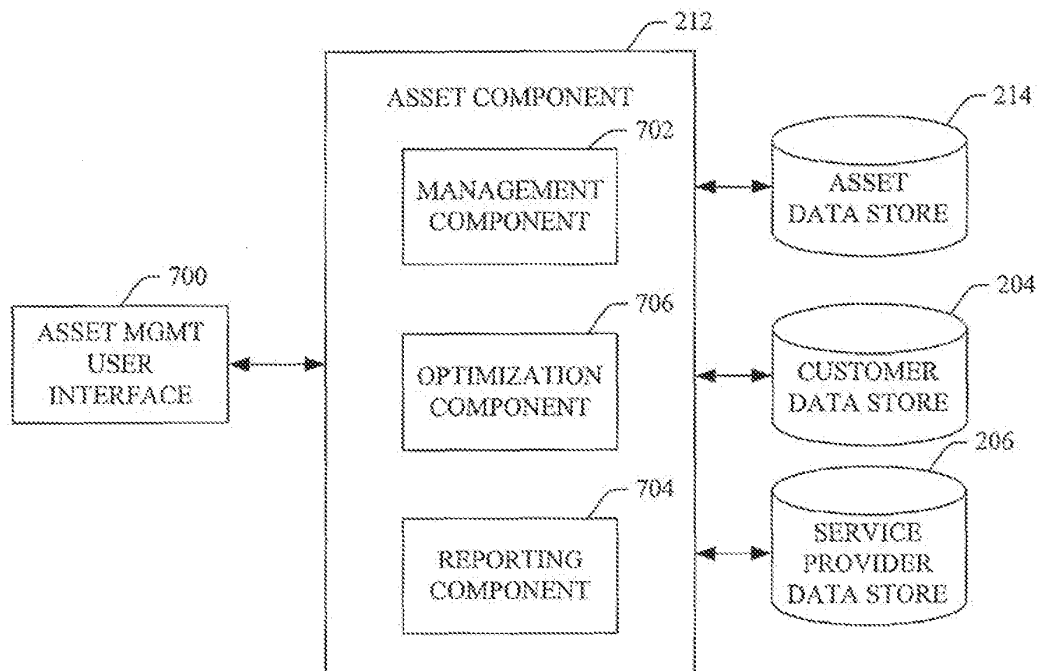


FIG. 7

8/17

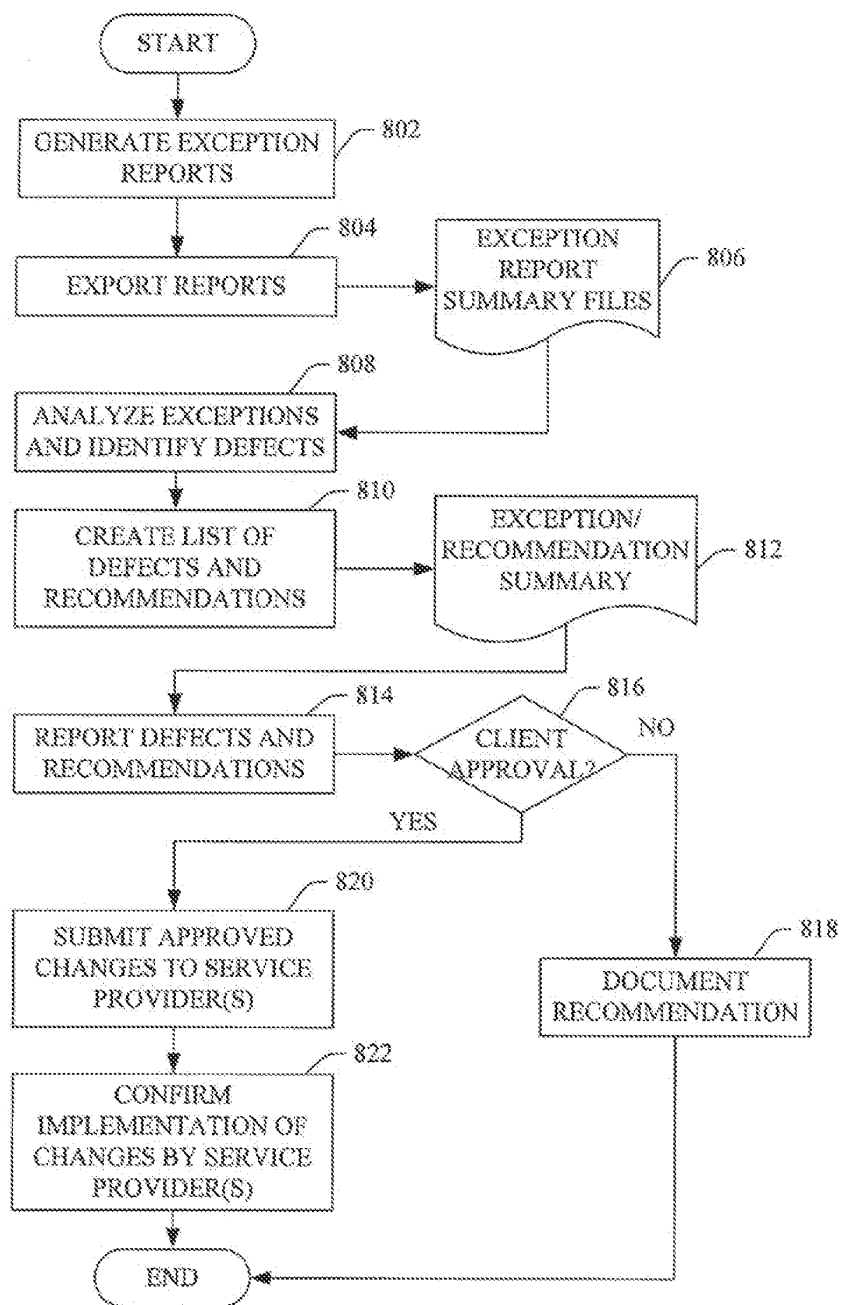


FIG. 8

9/17

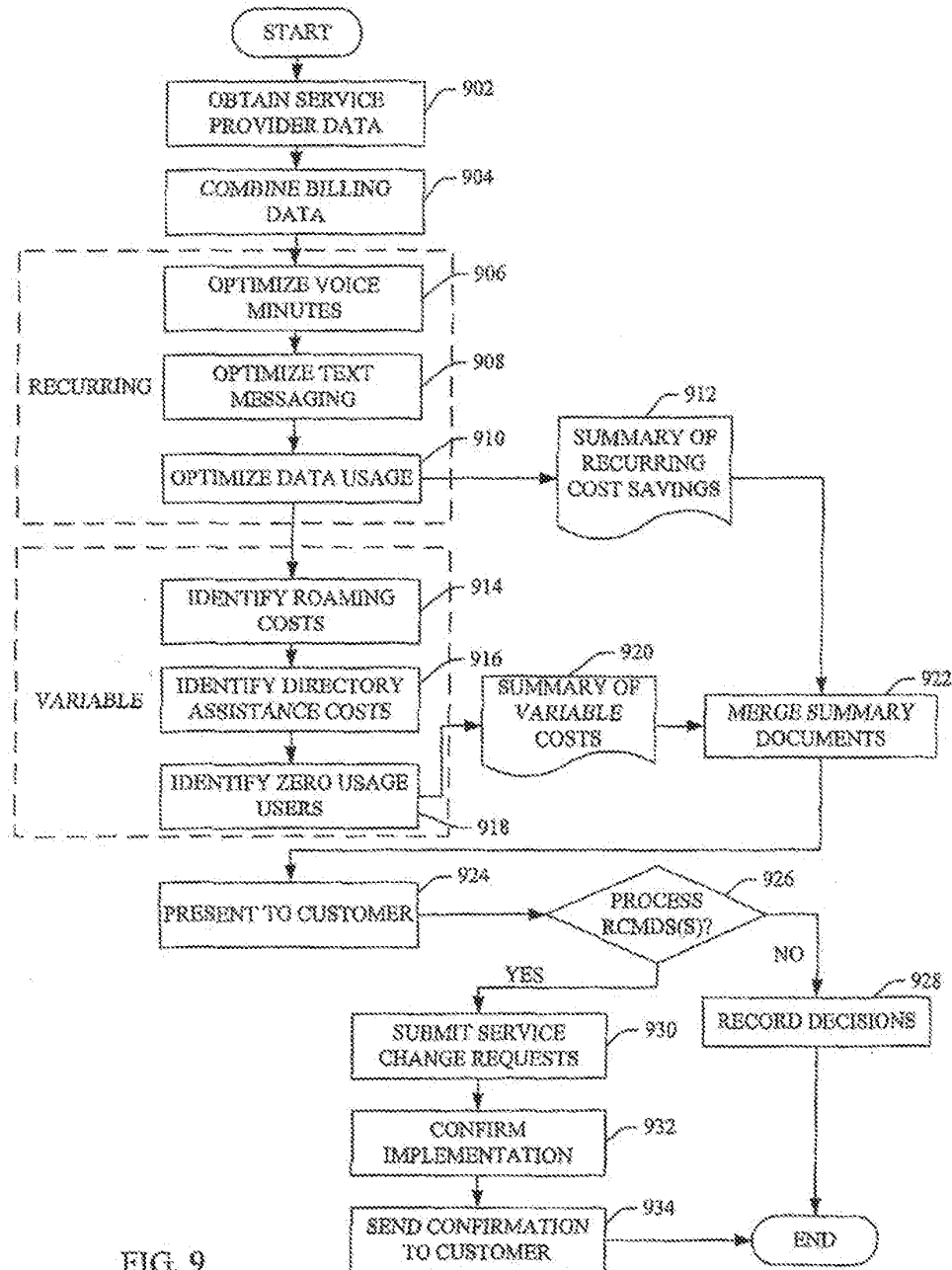


FIG. 9

10/17

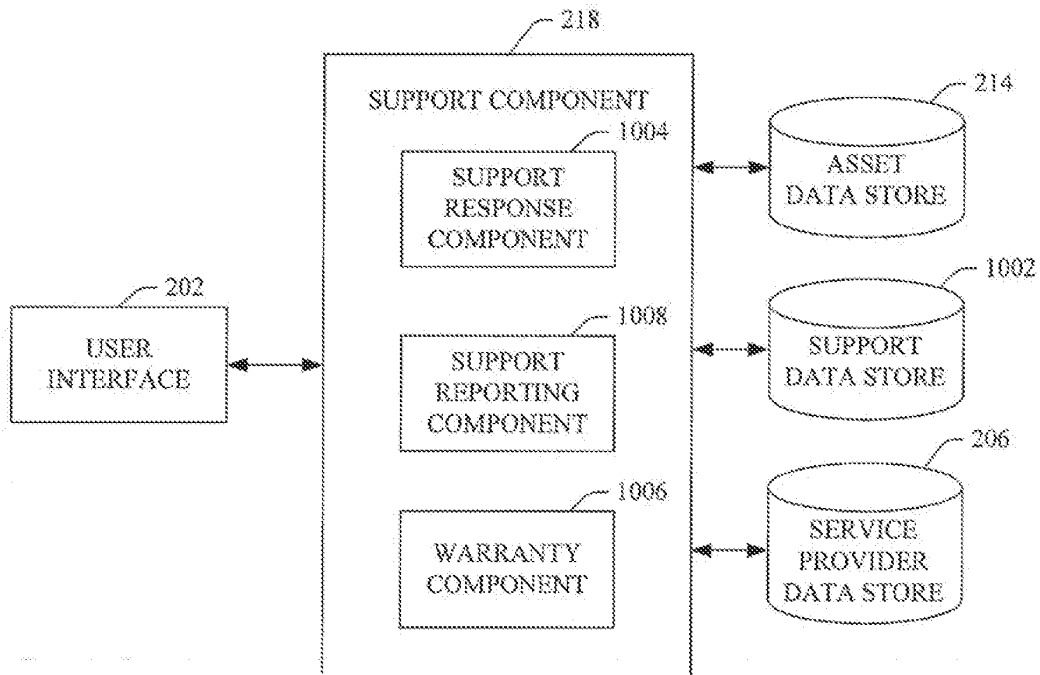


FIG. 10

11/17

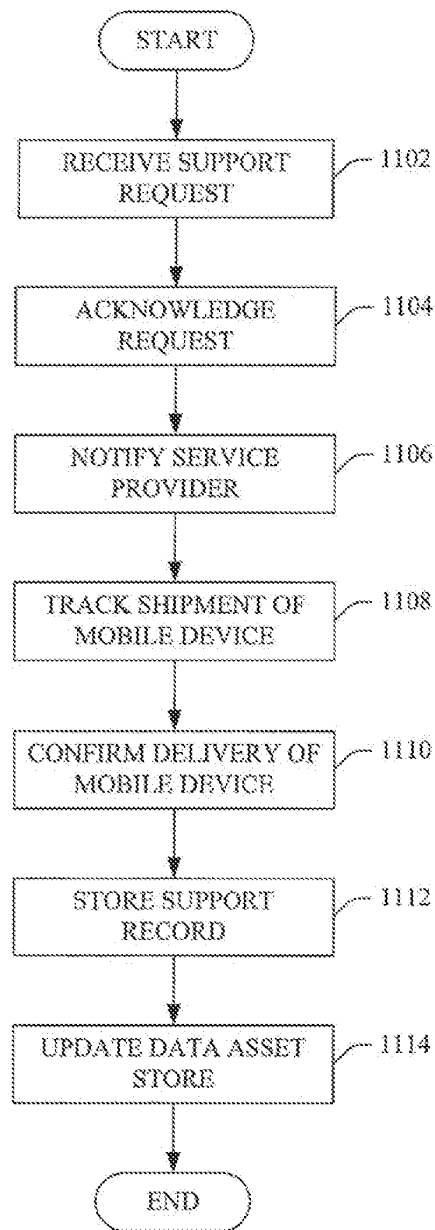


FIG. 11

12/17

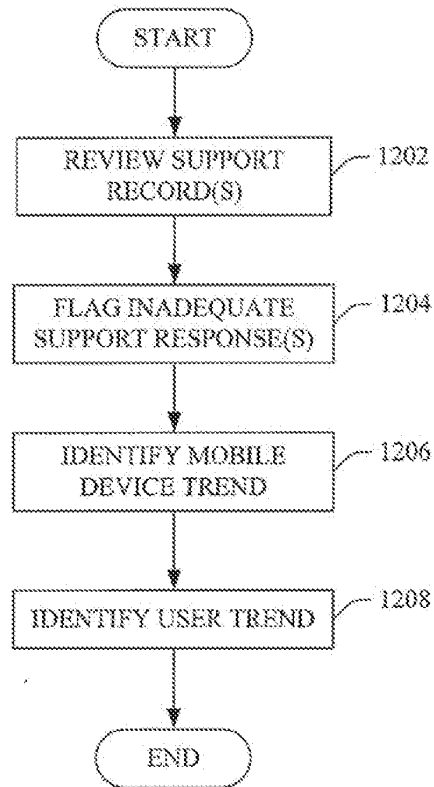


FIG. 12

13/17

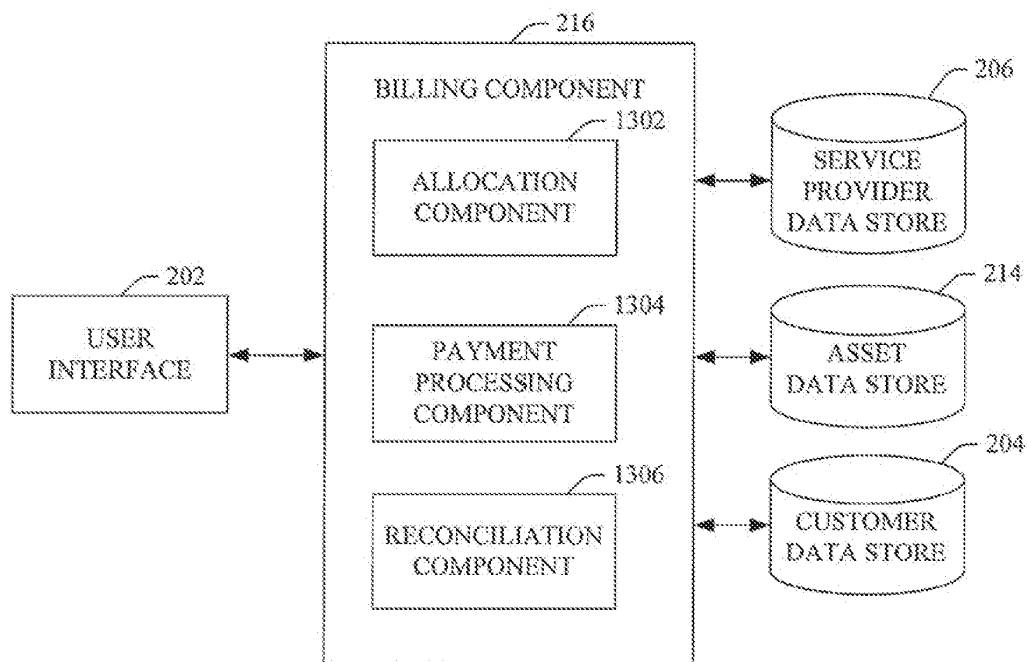


FIG. 13

14/17

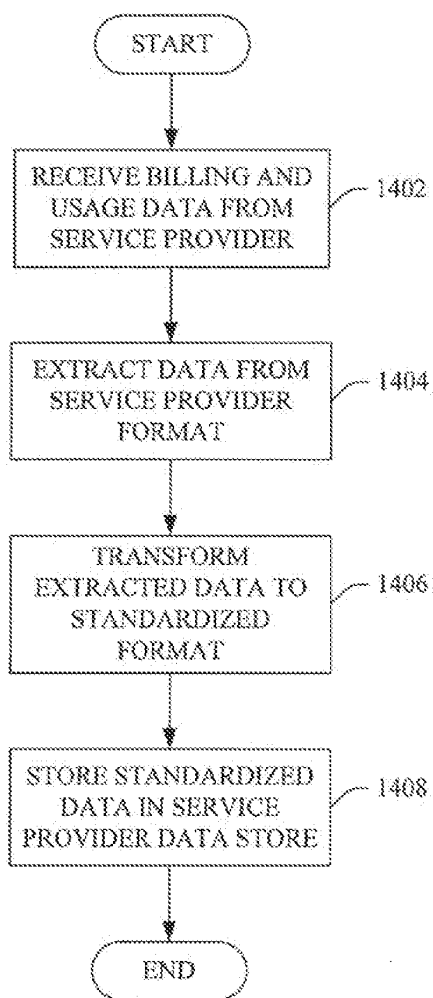


FIG. 14

15/17

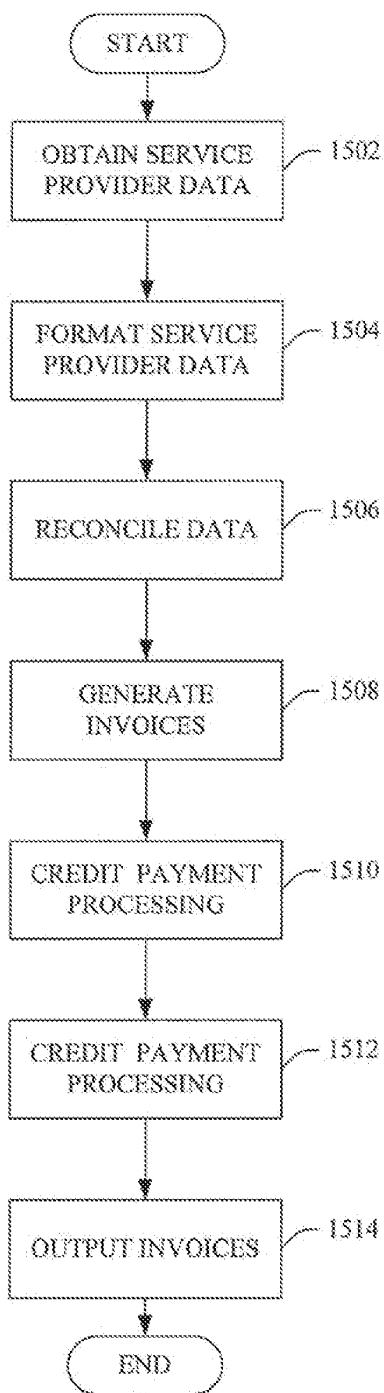


FIG. 15

16/17

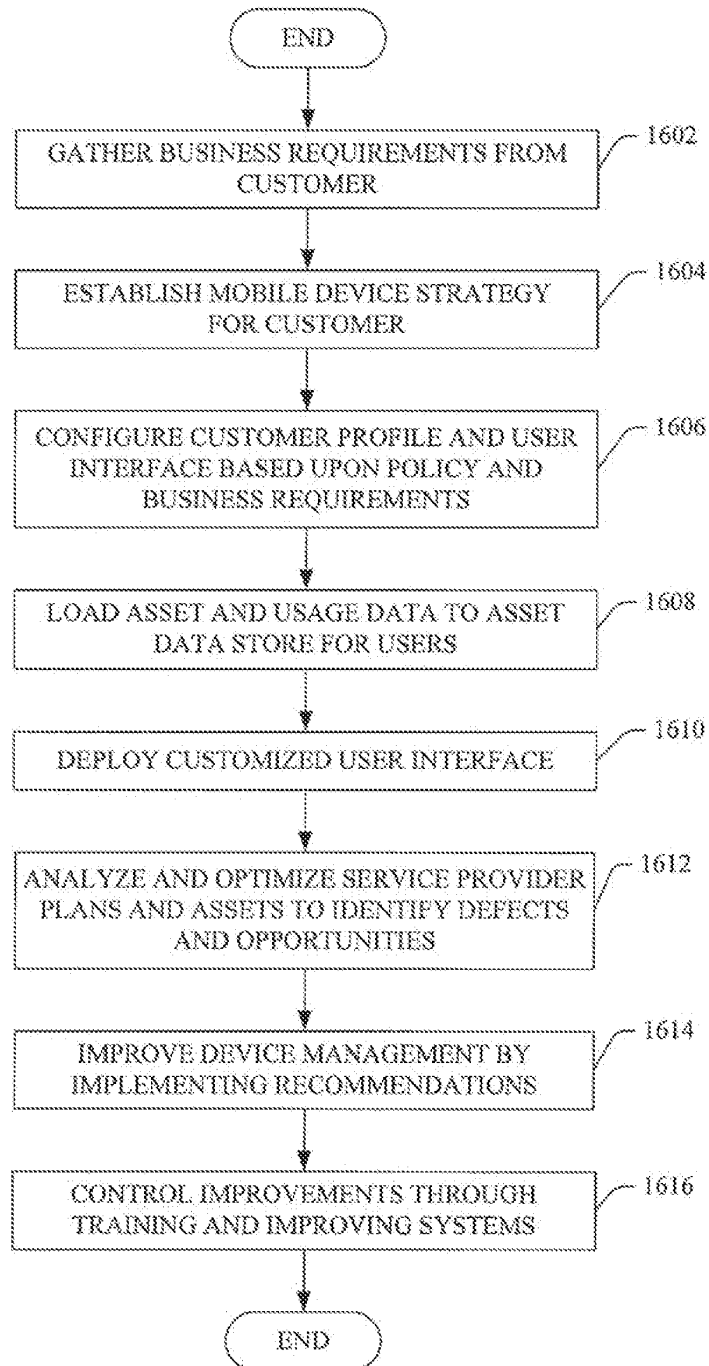


FIG. 16

17/17

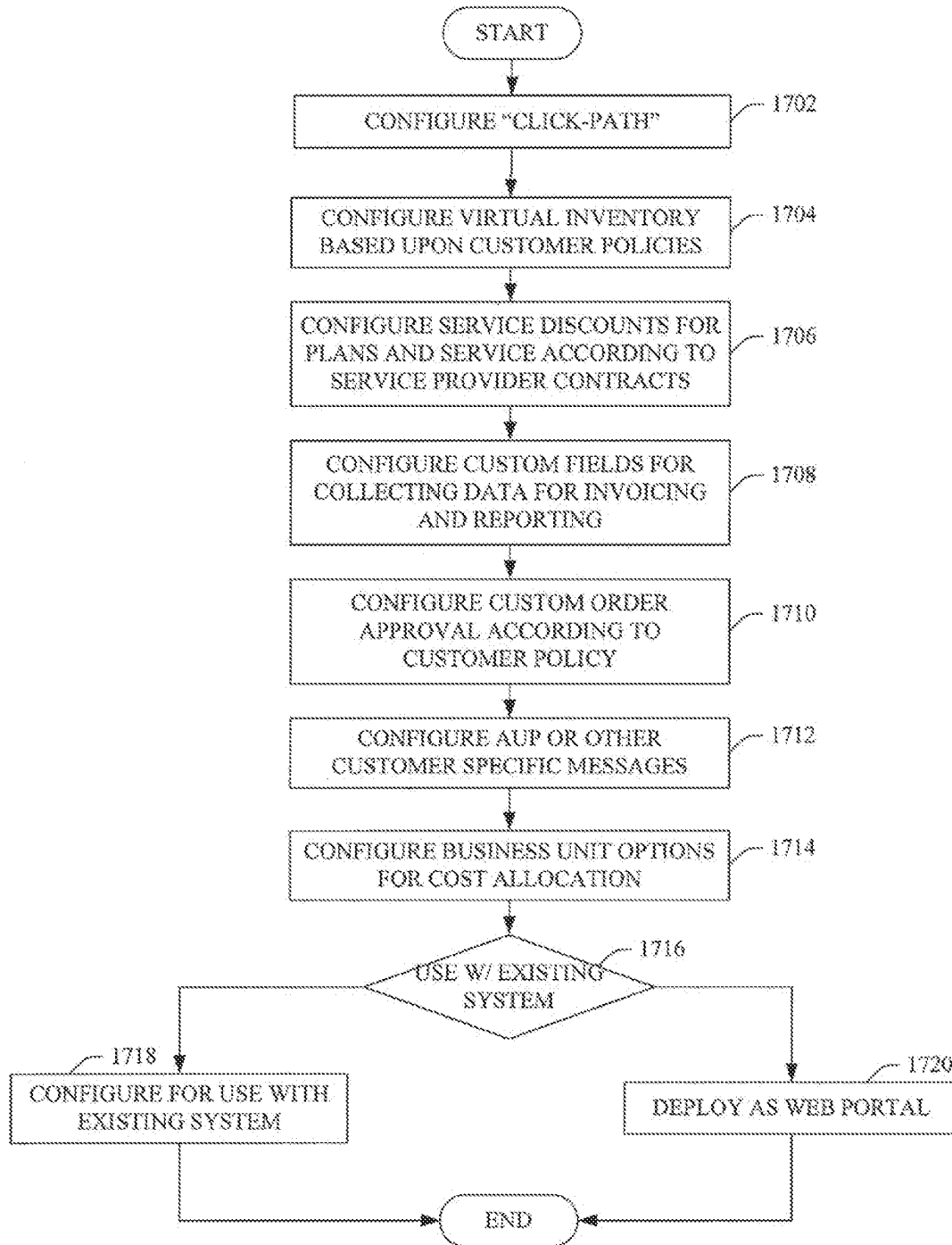


FIG. 17

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) PubWeb (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	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
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 "Z" document member of the same patent family		
Date of the actual completion of the international search 11 April 2008 (11.04.2008)		Date of mailing of the international search report 01 MAY 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201		Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4500 PCT Fax: 571-273-7774

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

(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 Classification: **H04M**
(21) International Application Number:
PCT/US2004/005252
(22) International Filing Date: 23 February 2004 (23.02.2004)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data:
60449,907 25 February 2003 (25.02.2003) US

(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, EG, 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, EG, 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

(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 Greyhinch Road, Andover, MA 01810 (US). RUDSILL, Luther; 6804 Poon Drive, Parker, TX 75002 (US).
(74) Agents: LEBOVICI, Victor, B. et al.; Weingarten, Schurgen, 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.

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

5 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.

10

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR
DEVELOPMENT

N/A

15

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.

20

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

25
30

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
5 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
10 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
15 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
20 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
25 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
30 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:

5 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;

10 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

15 Fig. 6 is a flow chart depicting the processing of outgoing calls.

DETAILED DESCRIPTION OF THE INVENTION

20 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, 25 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 30

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.

5 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
10 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
15 functionality, which are listed below:

1. Supervisory Control System service subscription and provisioning.
2. User profile configuration
3. Event control

20

These functional capabilities are discussed in greater detail below.

25 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
30 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;
- 5 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.

10 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
15 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
20 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
25 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.

30 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.

5 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
10 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
15 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
20 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
25 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
30 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

10

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 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.

10

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.

30

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.

5 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
10 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
15 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
20 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
25 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
30 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.

5 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
5 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
10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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.

20 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
25 identifiers. If the cell sector identifier of the calling party's phone corresponds to a restricted cell sector identifier 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
30 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
5 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
10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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
20 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
25 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
30 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
5 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.
10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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
20 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
25 communicated from the access point to the User Profile Database 32. For example if the Supervisor's user name is "abodef" 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-
30 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
5 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.

10 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
15 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
20 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
25 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
30 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.

5 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.

20 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.

30 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.

5 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
10 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
15 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.

20 4. Supervisory Control System Operation

4a. Supervisory Control System Operation for Incoming Calls to a User

 Operation and signaling for the Supervisory Control
25 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
30 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
5 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.

10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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.
20 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
25 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
30 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
5 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.

10 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
15 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
20 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
25 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
30 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.

5 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.

10 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
15 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
20 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
25 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
30 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.

10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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
20 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
25 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.
30 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
5 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
10 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
15 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
20 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
25 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
30 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
5 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.
10 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
15 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:

20 (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
25 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.

30 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.

30 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
5 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
10 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
15 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
20 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
25 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
30 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
5 and spirit of the appended claims.

CLAIMS

What is claimed is:

1. A method of controlling the usage of a wireless device
5 comprising the steps of:

obtaining a first set of coordinates in a specified
coordinate system representative of a first geographic
location;

- 10 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
15 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

- 20 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.

25

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.

30

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.

5

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.

10
15

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.

20

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.

25

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

30

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
5 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

10 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
15 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.

20

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
25 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
30 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.

5

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

10 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;

15 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.

20 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
25 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
30 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.

5

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.

10

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
15 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
20 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:
25 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

30 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

5 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.

10

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;

15

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

20

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
25 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
30 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
5 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
10 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
15 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;

20 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
25 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.

30

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
5 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
10 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
15 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.

20 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.

25

28. The system of claim 27 wherein said location identifier
comprises an address.

29. The system of claim 27 wherein said converter comprises a
30 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
5 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
10 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

15 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
20 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
25 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.

30 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

5 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

10 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;

15 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

20 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;

25 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

30 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
5 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
10 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
15 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
20 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
25 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
30 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.

5

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

10 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
15 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
20 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:

25 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

30 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
5 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.

10 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
15 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
20 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;
25 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
30 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;

5 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

10 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.

15 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
20 comprising:

 a second server operable to execute a supervisory process for controlling usage of said wireless phone as an overlay to said billing process;

25 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:

30 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

5 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
10 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.

15 48. The system of claim 45 wherein said predetermined period comprises a calendar month and said value comprises a specified number of minutes.

20 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
25 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
30 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
5 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;

10 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
15 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
20 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
25 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
30 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
5 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
10 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
15 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
20 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
25 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
30 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
5 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
10 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

15 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
20 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:

25 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
30 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
5 said at least one computer.

55. A method of communicating information regarding the usage of a wireless device comprising the steps of:

10 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;

15 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;

20 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

25 in the event said determining step indicates that said alert condition has occurred, communicating an alert message to said supervisor.

30 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.

5

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.

10

59. The method of claim 58 further including the step of resetting said time measure at the beginning of each control period.

15

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.

20

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.

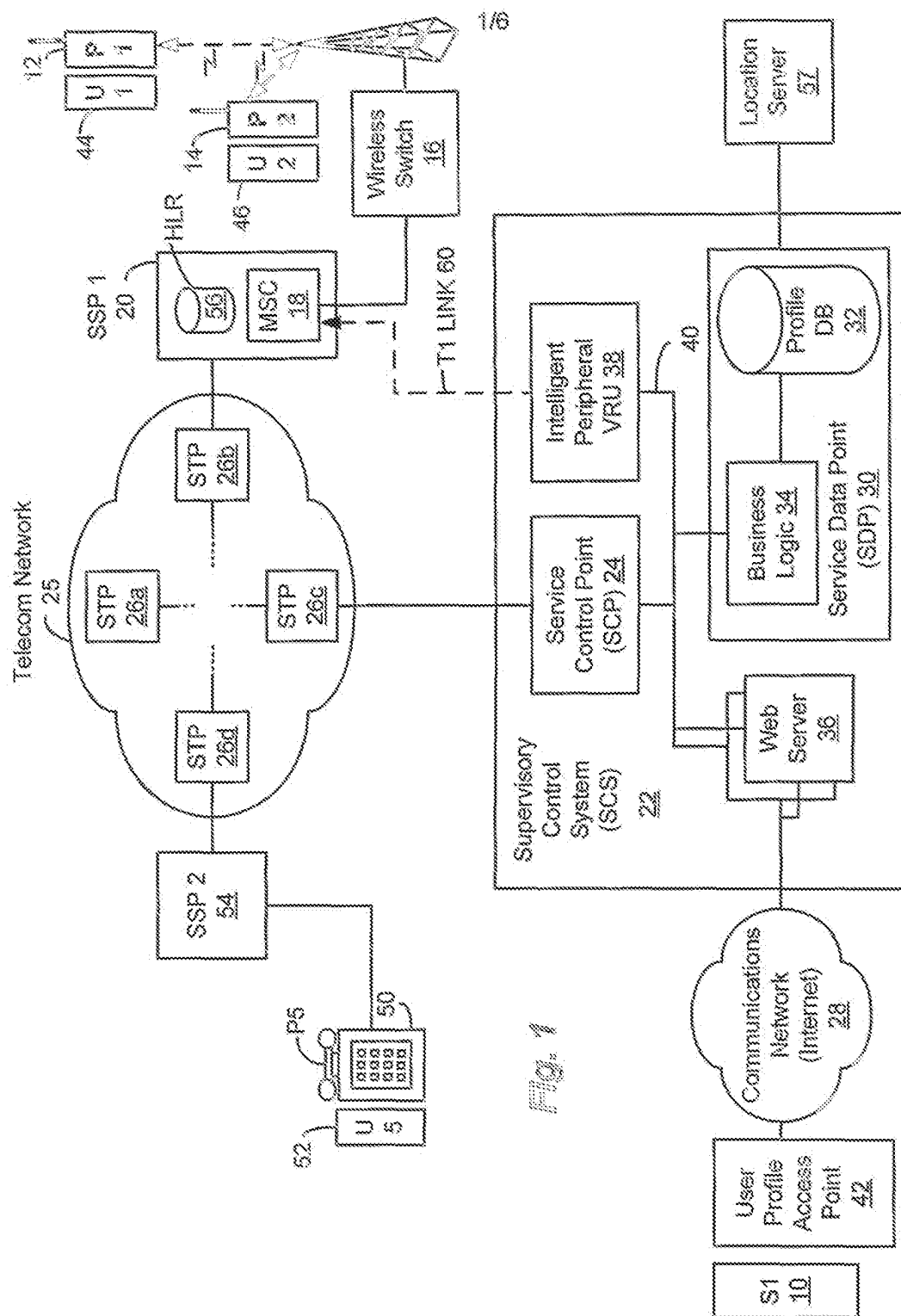
25

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.

30

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.



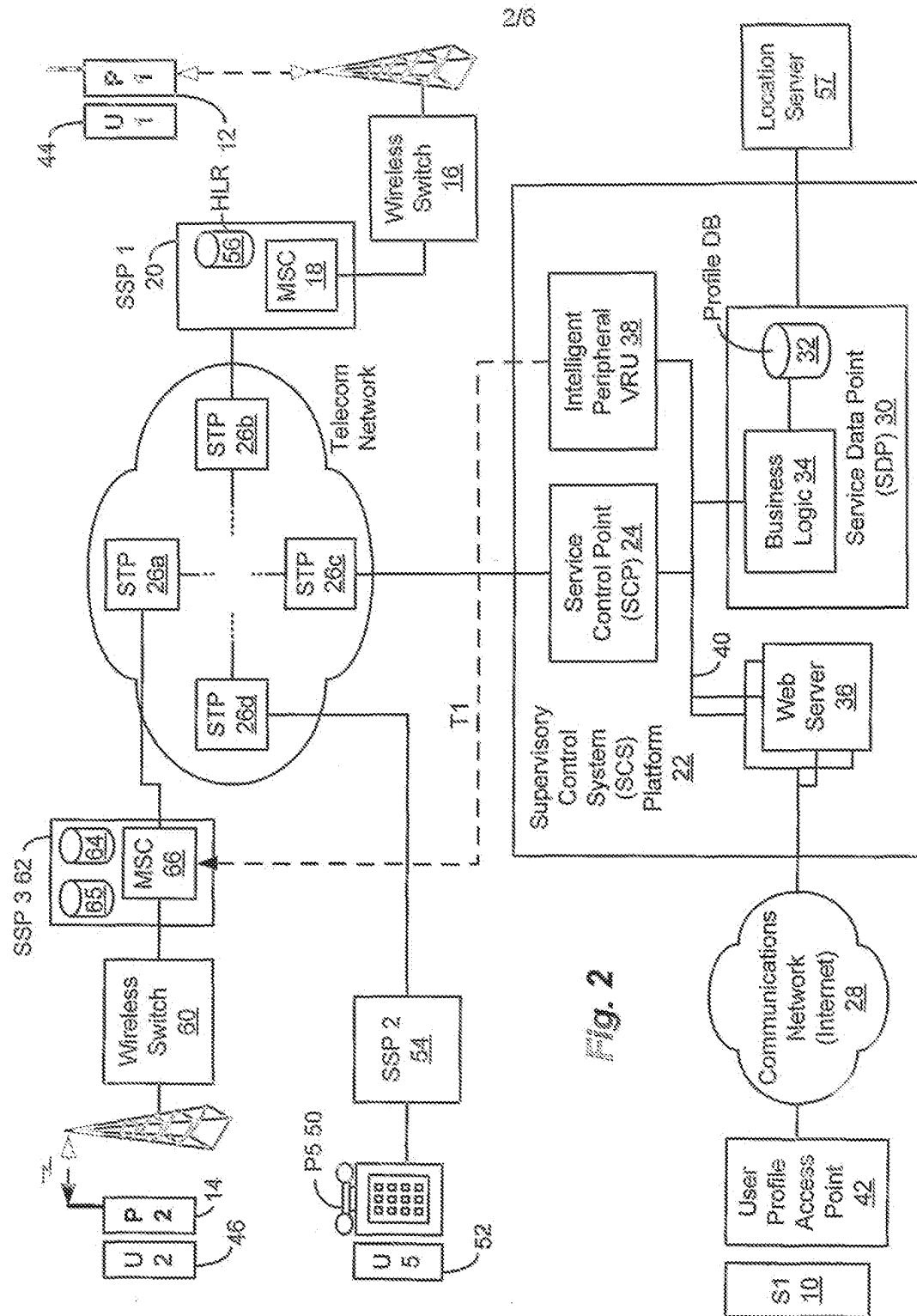
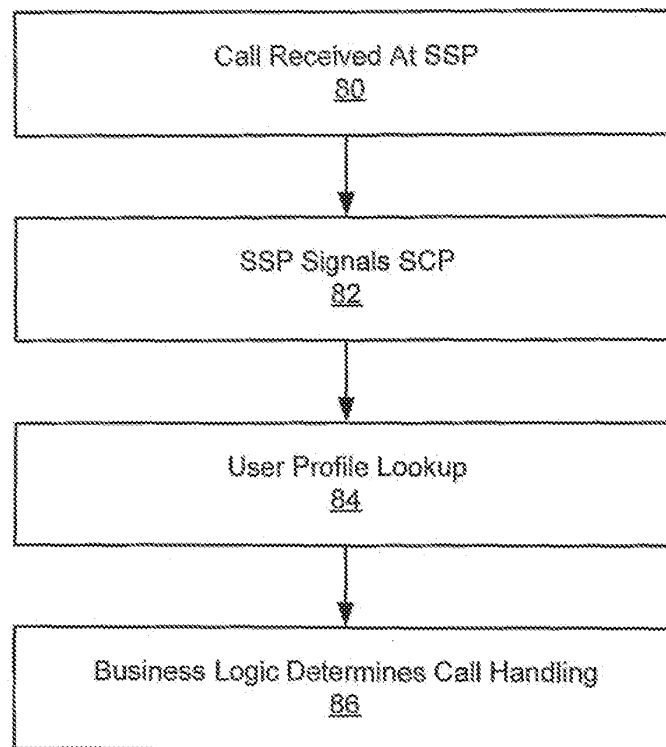
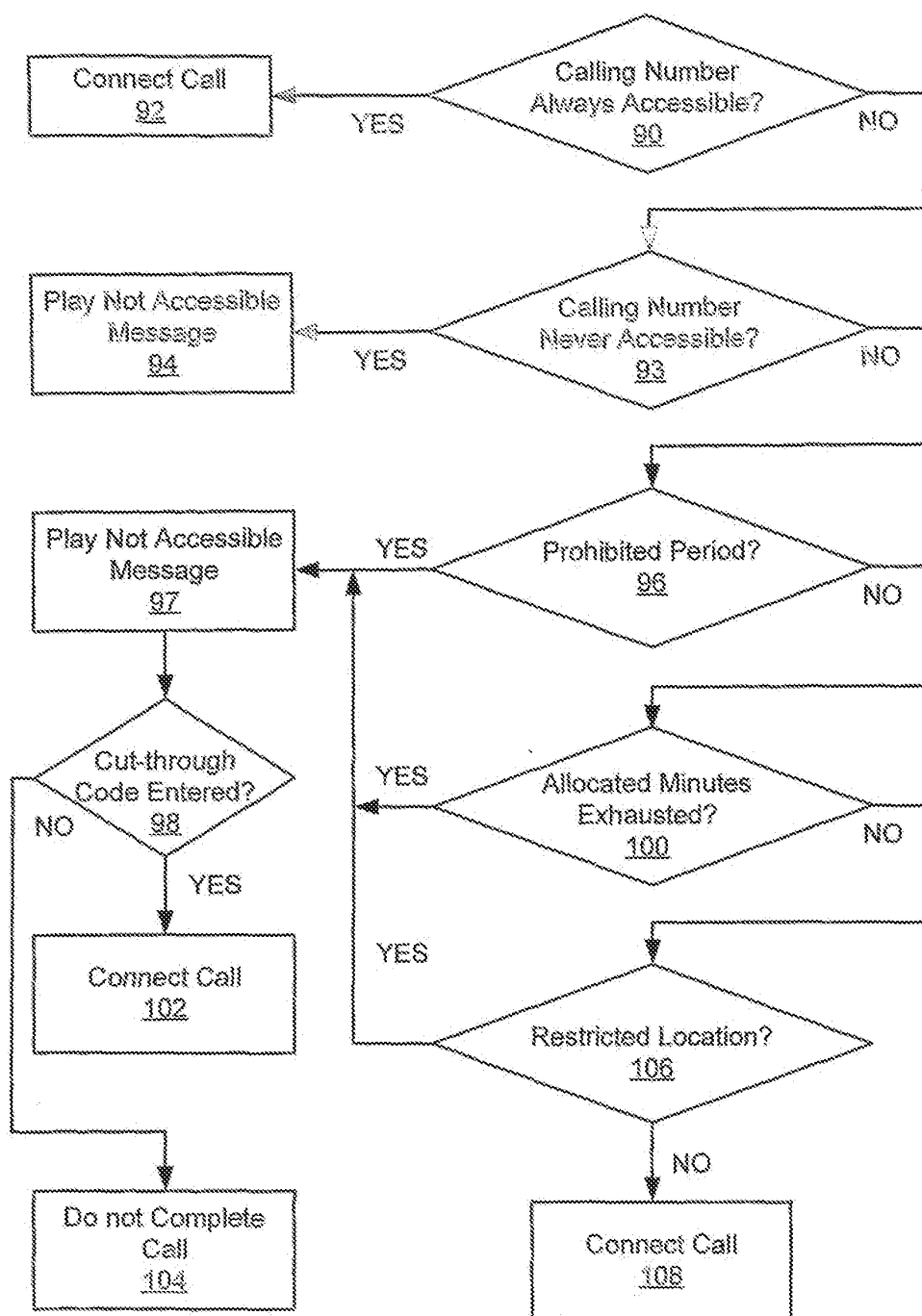


Fig. 2

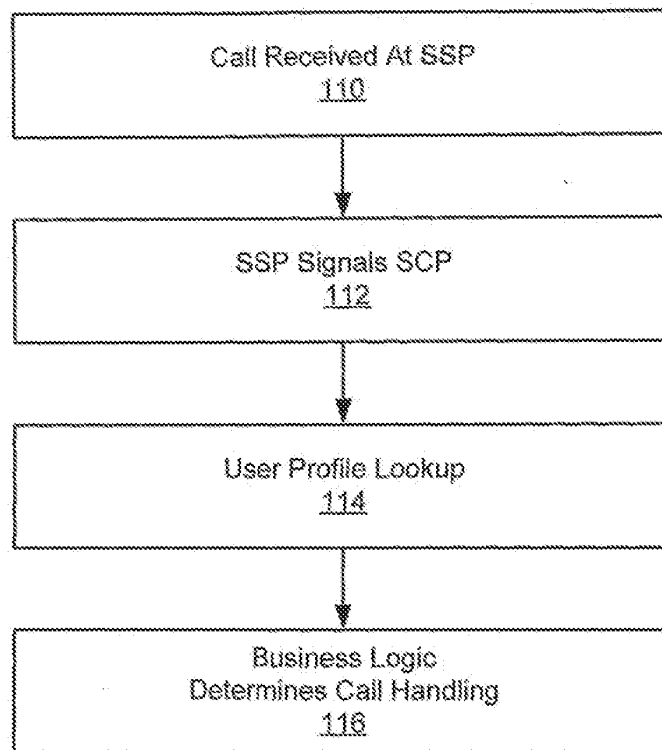
3/6

**Fig. 3**

4/6

**Fig. 4**

5/6

**Fig. 5**

535

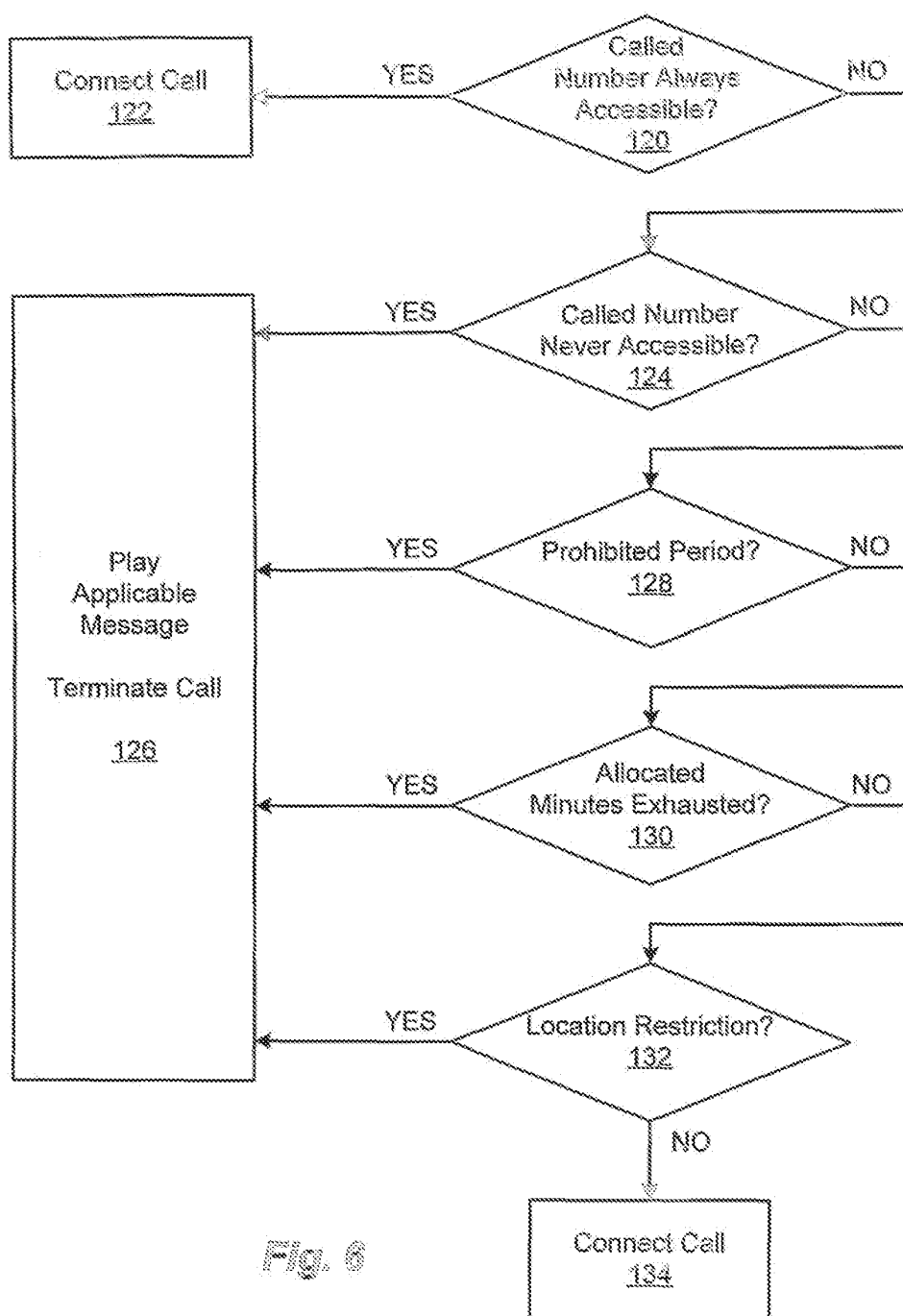


Fig. 6

(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 Classification⁷: **H04L 9/32**,
G07F 7/08

[SE/SE]: John Ericssonsgatan 16, S-652 22 Karlstad (SE).
KÅWE, Rolf [SE/SE]: Lingonstigen 7, S-654 68 Karlstad (SE).

(21) International Application Number: PCT/SE02/02424

(22) International Filing Date:
20 December 2002 (20.12.2002)

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0206061-0 10 January 2002 (10.01.2002) 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.

(71) Applicant (*for all designated States except US*): **TELIA AB (publ)** [SE/SE]; Mårbackagatan 11, S-123 86 Fursta (SE).

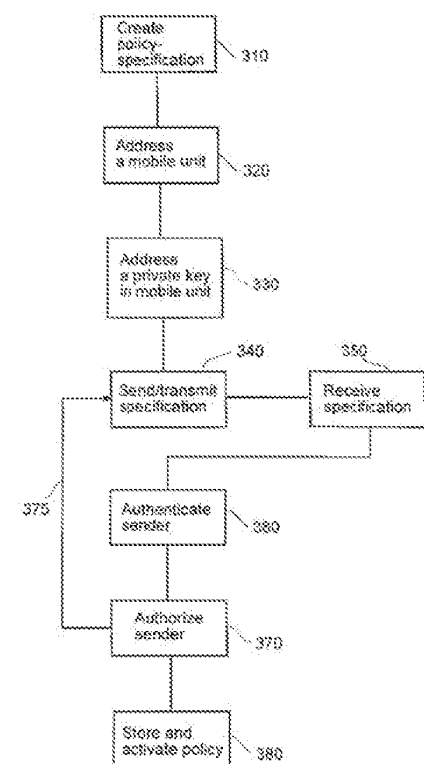
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, EG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

(72) Inventors: and

(75) Inventors/Applicants (*for US only*): **ERIKSSON, Jonas**

[Continued on next page]

(54) Title: METHOD OF 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 in 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, LI, 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

5 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
10 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
15 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.

20

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
25 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
30 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
35 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 is 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.

5 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
10 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
15 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
20 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
25 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

30 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
35 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
5 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
10 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
15 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
20 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
25 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
30 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.
- 35 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
5 105 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
10 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.

15 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
20 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
- 25 - 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
30 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
35 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-policies 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
5 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.

10 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
- 15 - write/read rights to/of data files
- GSM
- execution of applications
- etc.

20 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
25 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
30 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
35 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.

5 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
10 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.
15 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.

20

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, characterized in that said method includes the steps to
- 10 - 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
 - 15 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, characterized in the following steps:
- 20 - 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,
 - 25 - 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,
 - 30 - 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,
- 5 - 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,
- 10 - 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,
- 15 - ensuring that the specification is emanating from
approved gateway,
- storing of a policy which corresponds to the
specification, and
- activation of said policy.

20

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
25 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:

- 30 - 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-
35 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
5 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.
- 10 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.
- 15 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.
- 20 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.
- 25 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
30 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
35 arranged in a mobile unit.

13. A mobile communication system as claimed in any of the patent claims 7-12, characterized in that said policy specification is arranged in form of a data structure.

5

14. A mobile communication system as claimed in any of the patent claims 7-12, characterized in that said policy specification is arranged in form of an executable application.

10

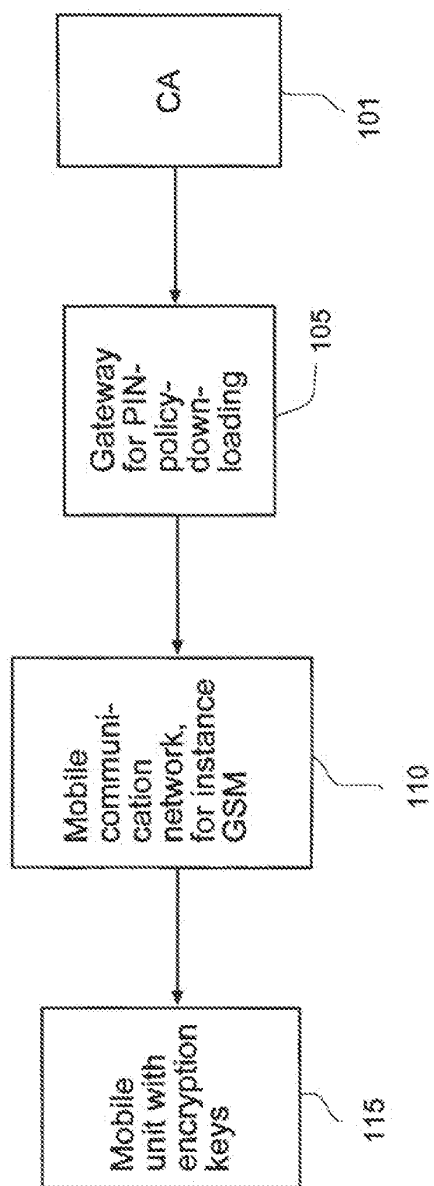


Figure 1

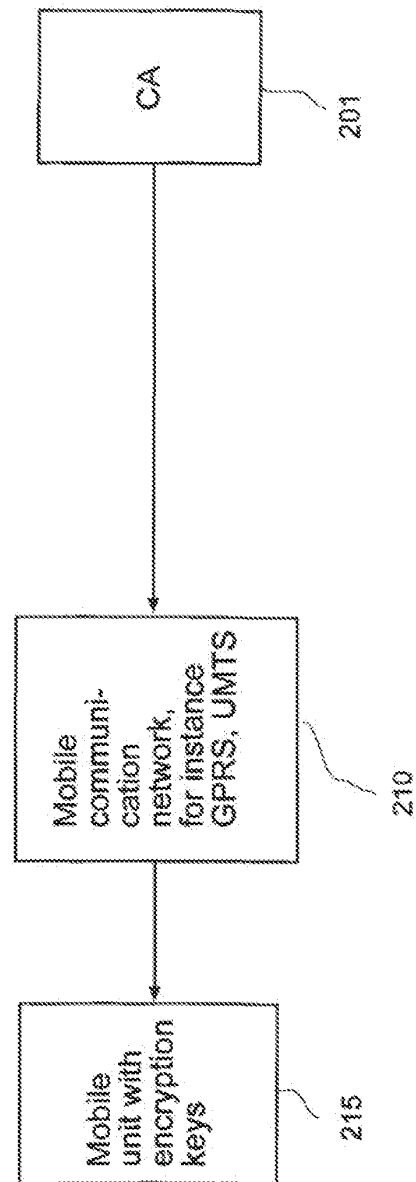


Figure 2

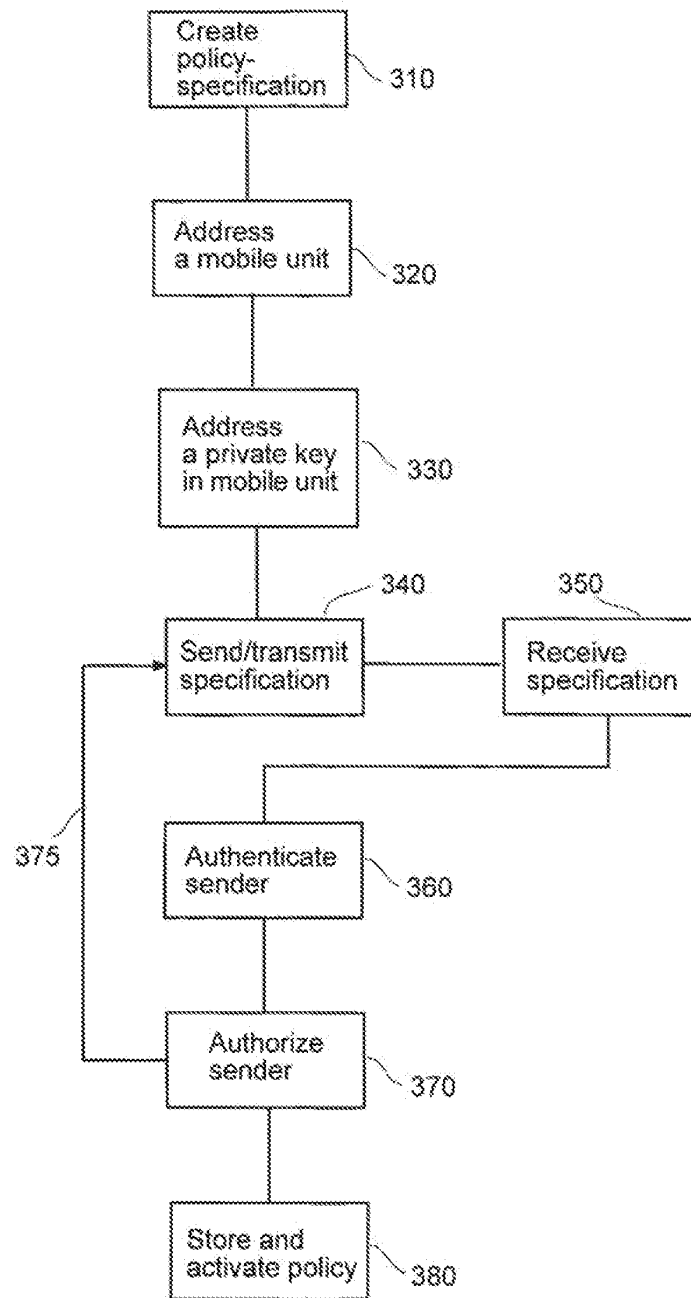


Figure 3

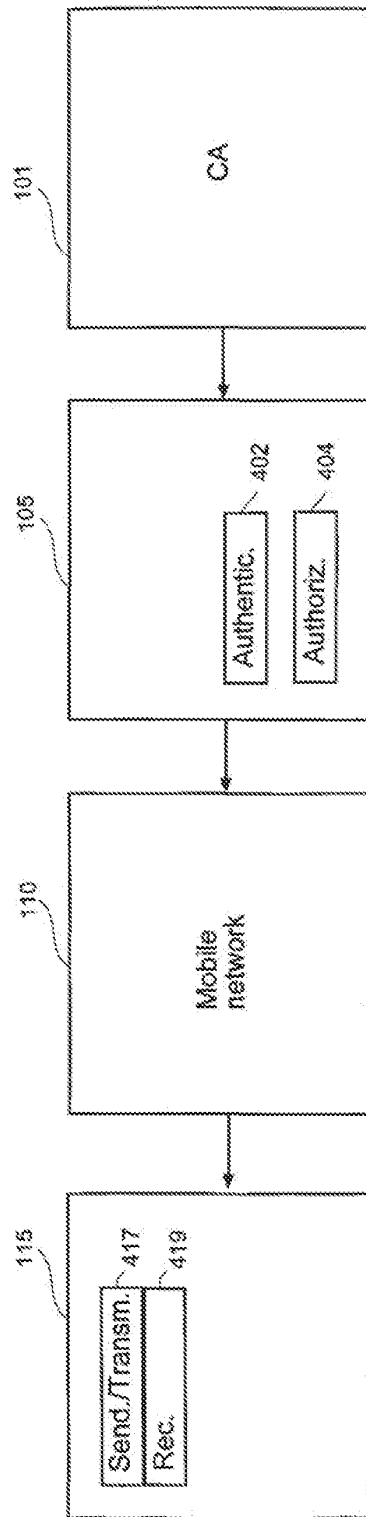


Figure 4A

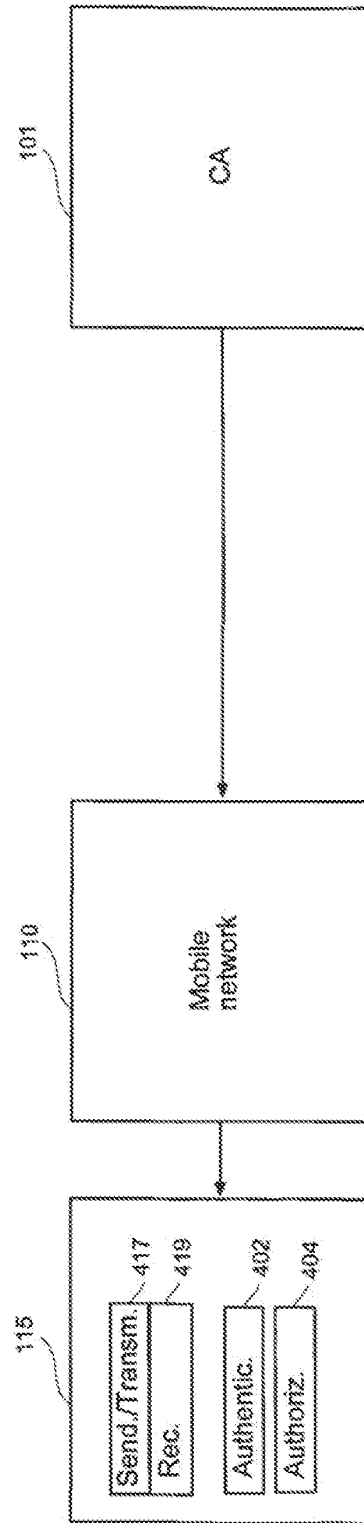


Figure 4B

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 (BROWNLIN, M. ET AL), 13 March 2001 (13.03.01), abstract, cited in the application ---	1-14
A	WO 0135685 A1 (MOBILIX A/S), 17 May 2001 (17.05.01), abstract, cited in the application ---	1-14
A	US 5944824 A (HE, J.), 31 August 1999 (31.08.99), claim 1 ---	1-14
A	US 4924514 A (MATYAS, S.M. ET AL), 8 May 1990 (08.05.90), cited in the application ---	1-14

☒ 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 combinations 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

7 April 2003

Date of mailing of the international search report

09-04-2003

Name and mailing address of the ISA/
Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Rune Bengtsson/mj

Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 02/02424

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0354771 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 14 February 1990 (14.02.90), abstract -----	1-14

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

28/02/03

International application No.
PCT/SE 02/02424

Patent document cited in search report			Publication date	Patent family member(s)		Publication date
US	6202157	B1	13/03/01	NONE		
WO	0135685	A1	17/05/01	AU	1269001 A	06/06/01
				BR	0015445 A	05/11/02
				DK	160899 A	10/05/01
				EP	1228653 A	07/08/02
US	5944824	A	31/08/99	NONE		
US	4924514	A	08/05/90	CA	1313411 A	02/02/93
				DE	68922884 D,T	30/11/95
				DE	68926005 D,T	17/10/96
				EP	0354771 A,B	14/02/90
				EP	0356065 A,B	28/02/90
				JP	2105192 A	17/04/90
				JP	2107722 C	06/11/96
				JP	8023736 B	06/03/96
EP	0354771	A2	14/02/90	CA	1317677 A	11/05/93
				DE	68922884 D,T	30/11/95
				DE	68926005 D,T	17/10/96
				DE	68926076 D,T	14/11/96
				DE	68926200 D,T	17/10/96
				EP	0354770 A,B	14/02/90
				EP	0354774 A,B	14/02/90
				EP	0356065 A,B	28/02/90
				JP	2099984 A	11/04/90
				JP	2105990 C	06/11/96
				JP	8020848 B	04/03/96
				US	4941176 A	10/07/90
				CA	1313411 A	02/02/93
				JP	2105192 A	17/04/90
				JP	2107722 C	06/11/96
				JP	8023736 B	06/03/96
				US	4924514 A	08/05/90

Form PCT/ISA/210 (patent family annex) (July 1998)

Electronic Acknowledgement Receipt	
EFS ID:	8300153
Application Number:	12694451
International Application Number:	
Confirmation Number:	6041
Title of Invention:	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM
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:	RALEP026
Receipt Date:	27-AUG-2010
Filing Date:	27-JAN-2010
Time Stamp:	16:13:50
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	RALEP026_IDS_Before_1st_OA.pdf	55737 d7b4cd4ac8d3f52b0b6d559498310b22ff34a013	no	2

Warnings:

Information:

2	Information Disclosure Statement (IDS) Filed (SB/08)	RALEP026_IDS_SB08_2.pdf	89834	no	2
			fa6b9d56fa28f1e3fd9997064ad31918e30419ba		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	RALE_Foreign_Ref_2A.pdf	5821505	no	34
			81bd528285eeb7055e34118b1c6f3ad0b406f580		
Warnings:					
Information:					
4	Foreign Reference	RALE_Foreign_Ref_2B.pdf	4014433	no	26
			6c150dbecf6e07e6e926c4953d9f7fa596419ee3		
Warnings:					
Information:					
5	Foreign Reference	RALE_Foreign_Ref_2C.pdf	8969766	no	61
			8a08a661fedb57f7c563ba498f498bb2309c2fc6		
Warnings:					
Information:					
6	Foreign Reference	RALE_Foreign_Ref_2D.pdf	12405145	no	79
			775980dffcf4fd87b178f106d99003d7a52ddaca2		
Warnings:					
Information:					
7	Foreign Reference	RALE_Foreign_Ref_2E.pdf	2436174	no	21
			c0f643662921a19d681c882cd985d04b7837a8bd		
Warnings:					
Information:					
8	NPL Documents	RALE_NPL_Ref_2F.pdf	219474	no	6
			ebce1f8721f1fe656f69a3905f36d944f0f575a4		
Warnings:					
Information:					
9	NPL Documents	RALE_NPL_Ref_2G.pdf	682711	no	77
			8ee373cfd5a9d752aae23b4ea2fc1e12b949497c		
Warnings:					
Information:					
10	NPL Documents	RALE_NPL_Ref_2H.pdf	137925	no	8
			312ccd04271430ed42b709573c0105d48599e5d		

Warnings:					
Information:					
11	NPL Documents	RALE_NPL_Ref_2I.pdf	1378815	no	17
			1d1b86ccc61e4d602380d993e4561849720eab8b		
Warnings:					
Information:					
12	NPL Documents	RALE_NPL_Ref_2J.pdf	1319237	no	5
			50d69a59a8af2531967879de03d70ef081cd46f2		
Warnings:					
Information:					
13	NPL Documents	RALE_NPL_Ref_2K.pdf	384366	no	23
			ca4acdc0719ea1636b3d667e2aafd3397dfca7ef		
Warnings:					
Information:					
14	NPL Documents	RALE_NPL_Ref_2L.pdf	3636374	no	15
			8440928107fdb5d75ce06783a2192520dc545702		
Warnings:					
Information:					
15	NPL Documents	RALE_NPL_Ref_2M.pdf	887279	no	111
			5a30977e77dc57a16d92c2240fea93e245299f94		
Warnings:					
Information:					
16	NPL Documents	RALE_NPL_Ref_2N.pdf	2190991	no	219
			8ba9616337a9da73d1158dfaec561ac7bc23b576		
Warnings:					
Information:					
17	NPL Documents	RALE_NPL_Ref_2O.pdf	22848329	no	262
			5dfb6b37b9bdba2974aea1f1643a2cc9b9129f17		
Warnings:					
Information:					
18	NPL Documents	RALE_NPL_Ref_2P.pdf	496028	no	35
			a267ff12b9b336818993ff8b85da8e35a5708cc5		
Warnings:					
Information:					
19	NPL Documents	RALE_NPL_Ref_2Q.pdf	1970806	no	10
			2398c7ca475eec3e037b4ad60021644397a754ed		

Warnings:					
Information:					
20	NPL Documents	RALE_NPL_Ref_2R.pdf	347340	no	11
			e87bfc75fa6949a4c1ea09d431b076cdc1b55249		
Warnings:					
Information:					
Total Files Size (in bytes):			70292269		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Gregory G. Raleigh	Examiner:	Not Assigned
Application No.:	12/694,451	Art Unit:	2617
Filed:	January 27, 2010	Docket No.:	RALEP026
Title:	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM		

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. RALEP026).

Application Serial No.: 12/694,451
Attorney Docket No. RALEP026

Page 1 of 2

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
12/694,451	01/27/2010	Gregory G. Raleigh	RALEP026

CONFIRMATION NO. 6041

21912

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

PUBLICATION NOTICE



OC000000042916200

Title:DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM

Publication No.US-2010-0197267-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 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
12/694,451	01/27/2010	2617	1480	RALEP026	25	3

CONFIRMATION NO. 6041

UPDATED FILING RECEIPT



OC000000041273919

21912

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

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 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009

Foreign Applications

If Required, Foreign Filing License Granted: 02/05/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/694,451**

Projected Publication Date: 08/05/2010

Non-Publication Request: No

Early Publication Request: No

page 1 of 3

Title

DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM

Preliminary Class

455

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

page 2 of 3

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

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

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

NOT GRANTED

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Gregory G. Raleigh	Examiner:	Not Assigned
Application No.:	12/694,451	Art Unit:	2617
Filed:	January 27, 2010	Docket No.:	RALEP026
Title:	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM		

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 16, 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				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. RALEP026).
- ☒ 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. RALEP026).
- ☒ 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. RALEP026

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: **DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM**, the specification of which,

- (check one)
1. ☐ is attached hereto.
 2. ☒ was filed on January 27, 2010 as
U.S. Application No. 12/694,451
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?

_____	_____	_____	☐ Yes ☐ No
(Appl. No.)	(Country)	(Filing Date)	

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)

<u>61/206,354</u>	<u>1/28/2009</u>
(Application No.)	(Filing Date)
<u>61/206,944</u>	<u>2/4/2009</u>
(Application No.)	(Filing Date)

61/207,393 2/10/2009
(Application No.) (Filing Date)

61/207,739 2/13/2009
(Application No.) (Filing Date)

61/270,353 7/6/2009
(Application No.) (Filing Date)

61/252,153 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 3/2/2009 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:	<u>4/8</u> , 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:	12694451			
Filing Date:	27-Jan-2010			
Title of Invention:	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM			
First Named Inventor/Applicant Name:	Gregory G. Raleigh			
Filer:	Michael J. Schallop/Veronica Pula			
Attorney Docket Number:	RALEP026			
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:	7429539
Application Number:	12694451
International Application Number:	
Confirmation Number:	6041
Title of Invention:	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM
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:	RALEP026
Receipt Date:	16-APR-2010
Filing Date:	27-JAN-2010
Time Stamp:	17:11:17
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	3735
Deposit Account	500685
Authorized User	
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)</p>	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	RALEP026_Response_to_Missing_Parts.pdf	83607 040a410b4627f508057ecb49db9bdcf1b8870ef	no	2
Warnings:					
Information:					
2	Oath or Declaration filed	RALEP026_Declaration_POA.pdf	471191 32751767bd134609d7dfc529c34c210a5afcd85b	no	2
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	38186 b93be4f4cc2f6a987e070b40977135ed5f0bb4d0e	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			592984		
<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>					



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
12/694,451	01/27/2010	Gregory G. Raleigh	RALEP026

CONFIRMATION NO. 6041

FORMALITIES LETTER

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



0000000040054378

Date Mailed: 02/16/2010

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.

/mkoroma/

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 1459
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
12/694,451	01/27/2010	2617	0.00	RALEP026	25	3

CONFIRMATION NO. 6041

21912

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

FILING RECEIPT



OC000000040054377

Date Mailed: 02/16/2010

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 61/270,353 07/06/2009
and claims benefit of 61/252,153 10/15/2009

Foreign Applications

If Required, Foreign Filing License Granted: 02/05/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/694,451**

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

Non-Publication Request: No

Early Publication Request: No

Title

DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM

Preliminary Class

455

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

page 2 of 3

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

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

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

NOT GRANTED

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

Attorney Docket No. RALEP026

APPLICATION FOR UNITED STATES PATENT

DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM

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

DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM

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, U.S. Provisional Patent Application No. 61/270,353 (Attorney Docket No. RALEP022+) entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING filed on July 6, 2009, and U.S. Provisional Patent Application No. 61/252,153 (Attorney Docket No. RALEP026+) entitled DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM filed on October 15, 2009, which are incorporated herein by reference for all purposes.

[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 wireless network architecture for providing device group partitions and a settlement platform in accordance with some embodiments.

[0007] **Figure 2** illustrates another wireless network architecture for providing device group partitions and a settlement platform in accordance with some embodiments.

[0008] **Figure 3** illustrates a wireless network architecture including a settlement platform in accordance with some embodiments.

[0009] **Figure 4** illustrates a flow diagram for providing device assisted service usage information in accordance with some embodiments.

[0010] **Figure 5** illustrates a flow diagram for providing a settlement platform service in accordance with some embodiments.

DETAILED DESCRIPTION

[0011] 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.

[0012] 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.

[0013] In some embodiments, device group partitions (e.g., partitions of devices based on associated device groups) are provided, as described herein. For example, one or more device service processor settings are controlled by a service controller, which can be partitioned to allow groups of devices (e.g., device group partitions, such as based on type of device, service plan (such as a service plan that is based on a revenue share and/or any other service plan), geography, service provider, enterprise, user group, or based on any other criteria for grouping

devices) to be securely controlled. In some embodiments, a device group partition control capability is enabled by providing a secure network connection to the service policy settings tools that define the device pre-provisioning settings, the device pre-activation service profile settings, the network equipment service activity control policy settings (e.g., access control, routing policy, traffic control, usage limits, and/or policy for usage limit overage), and/or the network billing system database. By providing server tools that enable such settings to be controlled (e.g., or perhaps only observed, such as with respect to the billing system) by a secure workstation or secure website interface that provides network communication with the equipment, for example, that can be used to configure or program the settings, and providing for a secure partitioning of the devices that can be controlled by a given secure workstation or secure website interface, a central provider or a service provider can provide such services to, for example, multiple entities (e.g., an MVNO or an entity, such as a corporation or government agency, allocated a group of devices in a device group partition) that each can have different device and service plan combinations and/or different flavors of services for such devices (e.g., various ambient services, revenue sharing service models, and/or any other services/service plans or combinations thereof). In some embodiments, the networking equipment is implemented to secure device group partitions in which the service policies for a group of devices can be securely controlled.

[0014] In some embodiments, the service controller relies entirely on network based service usage measures to determine service usage for a given device, and aggregates or organizes device usage information for multiple devices that belong to a device group partition so that the usage activity for each device within the device group is logged for that device group. In some embodiments, the device service usage activity for each device group is then analyzed and summarized into a service activity report for that device group. In some embodiments, the device group service activity report thus generated is further processed with business logic rules to determine a service activity payment that is owed to a device group partner of a carrier, MVNO or other entity that owns of the service controller settings that determine the manner in which the device usage information is collected, aggregated, analyzed and further processed with business rules. For example, the device group partner can be an OEM, an ambient service partner, a roaming service partner, a carrier network partner, a service seller, a service re-seller, a service wholesaler, an MVNO, a virtual MVNO or other entity that has a business relationship

with the entity that owns the service controller settings and wishes to compensate the partner for helping in some way to distribute services or service activations.

[0015] In some embodiments, the business rules logic include a variety of reconciliation algorithms to determine a payment that is due to or from a device group partner. For example, the business rules logic can determine if a device has activated on a service plan and if so which service plan the device was activated on, and this information can be used to either pay an activation incentive payment to a device group partner or can be used to generate a revenue share payment for each billing period a service play is paid for by the user. Different activation incentive payments or revenue share payments can be made based on which service plan the user activated. For example, if a device activates with a 24 hour session based plan, the one payment can be due, if a device activates with monthly service plan another larger payment is due, and/or if a device activates with a 2 year contract plan then an even larger payment is due. Similarly, in a revenue share example, the revenue share for service usage on a 24 hour plan can be a relatively low revenue share payment, while the revenue share is higher for service usage associated with a monthly service plan and even higher for a longer term contract plan. In other examples, revenue share can also be a fixed percentage of the carrier revenue for a given service plan, with the percentage potentially changing for different service plans. In another example, a user can activate on one service plan but then change to another service plan at a later time and in this case either an activation incentive payment or revenue share payment can be adjusted to reflect the change in service plan. In another example, not all the device service activity for devices within a device group is analyzed and/or provided to a device group service partner, but instead a portion of the device service activity can be analyzed and/or reported. An example where this is desirable is a situation in which an ambient service partner needs to know how much of the partner's ambient service usage was consumed by a device group for purposes of paying for that ambient service usage, but does not need to know or should not be provided with information about device usage for other ambient services or user service plan services. Another example is a device group service partner report that details service partner user purchase transactions only for the device group service partner's services and not for other possible device group service partners.

[0016] In some embodiments, the service controller relies at least in part on device based service usage measures to determine service usage for a given device, and aggregates or organizes device usage information for multiple devices that belong to a device group partition so that the usage activity for each device within the device group is logged for that device group.

[0017] In some embodiments, the aggregated service activity information for a given device group is made available to a service partner so that the service partner can audit service activity based payments. For example, this information can be made available through a Web UI, a secure web UI, other electronic distribution media or in hard copy format. In some embodiments, the aggregated service information for a device group is further processed with the business rules logic as described herein, and a summary report of service usage or service activation information is made available to the service partner. As similarly discussed herein, this information can be made available in a variety of electronic and/or hardcopy formats. In some embodiments, both the aggregate service usage information and the information that results from further processing with business rules logic are made available to a device group partner.

[0018] In some embodiments, a programming interface is provided to allow for programmable definition of the device group service usage information into a device group activity report and/or to allow for a programmable definition of the business rules to analyze the device group service activity reports and create a device group reconciliation report. In some embodiments, this programming interface is provided/implemented as a secure web UI or web portal that allows a device group manager to program the device activity collection rules and/or program the business rules logic used to create the reconciliation report. In some embodiments, the secure web UI includes a pre-defined UI that simplifies the process of writing device group service usage information aggregation filter rules and/or device group service activity information reconciliation filter (e.g., or business logic) rules. In some embodiments, a secure UI is provided so that a device group service partner is allowed to view all or part of the service activity aggregation rules and/or all or part of the reconciliation (e.g., or business logic) rules for the device group the partner is associated with.

[0019] In some embodiments, service usage information includes network based service usage information. In some embodiments, the network based service usage information includes

network based CDRs (Charging Data Records). In some embodiments, service usage information includes device based service usage information. In some embodiments, device based service usage information includes device assisted CDRs, also referred to herein as micro-CDRs, as described herein. In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired (e.g., providing granular service usage information, such as based on application layer service usage monitoring, transaction service usage monitoring, and/or other types of service usage information). In some embodiments, each device includes a service processor (e.g., a service processor executed on a processor of a communications device, such as a mobile device or an intermediate networking device that can communicate with a wireless network).

[0020] In some embodiments, each device activity that is desired to be associated with a billing event is assigned a micro-CDR transaction code, and the service processor is programmed to account for that activity associated with that transaction code (e.g., various transaction codes can be associated with service usage associated with Apple iTunes music, Apple App Store applications, FaceBook social networking, Google search, eBay online commerce, and Amazon Kindle eBooks, respectively, which can be used for providing granular service usage for these various Internet/network based services/sites/transactions and/or any other Internet/network based services/sites, which can include transactional based services, such as Apple iTunes, Apple App Store, and Amazon Kindle). For example, using these techniques, as described herein, essentially any type of device activity can be individually accounted for and/or controlled (e.g., throttled, restricted, and/or otherwise controlled as desired). In some embodiments, the service processor periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, a service controller or some other network element/function. In some embodiments, the service controller reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN or some other authorized network element/function for CDRs) and then transmits the reformatted micro-CDRs to a network element/function for performing CDR mediation.

[0021] In some embodiments, CDR mediation is used to properly account for the micro-CDR service usage information by depositing it into an appropriate service usage account and

deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions for CDR mediation and billing. For example, the billing system can process the mediated CDR feed from CDR mediation, apply the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generate billing events in a manner that does not require changes to existing billing systems, infrastructures, and techniques (e.g., using new transaction codes to label the new device assisted billing capabilities).

[0022] In some embodiments, the communications device is a mobile communications device, and the service includes one or more Internet based services, and 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. In some embodiments, the communications device includes a modem, and the processor is located in the modem. In some embodiments, an intermediate networking device includes any type of networking device capable of communicating with a device and a network, including a wireless network, example intermediate networking devices include a femto cell, or any network communication device that translates the wireless data received from the device to a network, such as an access network. In some embodiments, intermediate networking devices include 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems, DSL modems, remote access/backup routers, and other intermediate network devices.

[0023] In some embodiments, a revenue sharing model is provided using a settlement platform. In some embodiments, a revenue sharing model is provided using a settlement platform for providing one or more of the following: service activation revenue share or bounty (e.g., to one or more partners, such as OEMs, an ambient service partner, a roaming service partner, a carrier network partner, a device retailer or distributor, a service seller, a service reseller, distributors, MVNOs, carriers, and/or service providers), service usage billing (e.g., to one or more partners, such as OEMs, distributors, MVNOs, carriers, and/or service providers), service usage revenue share (e.g., to one or more partners, such as OEMs, distributors, MVNOs, carriers, and/or service providers), and transactional revenue share (e.g., to one or more partners, such as an OEM, an ambient service partner, a roaming service partner, a carrier network

partner, a device retailer or distributor, a service seller, a service re-seller, distributors, MVNOs, carriers, and/or service providers). For example, a revenue sharing model can allow for a distribution partner to access activation information for a specified device or a specified device group for which they are potentially entitled to a bounty (e.g., a fixed fee or some other payment or credit terms, etc.) for activation, and the revenue sharing model can also allow for one or more OEMs (e.g., or other device group partner) access to information regarding service usage for the specified device or the specified device group for which they are potentially entitled to a service usage revenue share (e.g., percentage, fixed fee, transactional fee or credit, or some other form of revenue share) for the associated or particular service usage. For example, a distributor (e.g., Amazon, Best Buy, or any other distributor) can be allocated a bounty for each activated eBook reader based on service activation for that eBook reader (e.g., the value/terms of the bounty can vary based on the type of service that is activated for that eBook reader, such as an ambient service versus a premium data plan service), and the bounty can also require activation within a certain period of time of the sale (e.g., if activated within 30 days after sale by the distributor of the eBook to a customer). As another example, a service revenue share can be provided with an OEM (e.g., Sony or Google, or another eBook manufacturer, or another device group distribution partner), for example, for a period of time after the initial activation of the eBook reader (e.g., 2 years after activation), which is referred to herein as, for example, a service revenue bounty, a service revenue share, or a service revenue sharing model. In some embodiments, a partner (e.g., Amazon, Barnes & Noble, Google, or any other partner) pays for or subsidizes the cost of the associated service usage for the eBook reader, and a revenue share for each book paid for by the service provider is provided (e.g., a transactional service revenue share) between the service provider (e.g., carrier, central provider, MVNO, and/or other service provider) and the partner. In some embodiments, these and other revenue share model techniques are implemented using a settlement platform, as described herein. In some embodiments, these and other revenue share and service billing techniques are implemented using a settlement platform and micro-CDRs, as described herein.

[0024] In some embodiments, a billing interface is provided between the service controller and the billing system (e.g., an external service plan read/write interface). In some embodiments, the service controller periodically polls the billing system interface with a request/command (e.g., "read-billing-plan" command) to determine if the user has changed the

service plan of choice through some interface other than the service processor service plan selection UI (User Interface) (e.g., Internet or phone). If the user has changed the service plan, then the service controller updates the service plan of record on the service controller database and on the device (e.g., via secure communication with the service processor executing on a processor of the device). In some embodiments, another request/command (e.g., the "write-billing-plan" interface command) is used to inform the billing system when the user has selected a new or initial plan option from the service processor service plan selection UI.

[0025] In some embodiments, a settlement platform is provided, as described herein. In some embodiments, the settlement platform includes support for an activation process (e.g., to facilitate tracking and payment of a bounty for one or more partners for an activation). In some embodiments, the settlement platform provides a service/transactional revenue share settlement platform. In some embodiments, the settlement platform distributes accounting and settlement information to one or more of carriers, distribution partners, MVNOs (Mobile Virtual Network Operator), wholesale partners, and/or other partners (e.g., for a service usage billing to one or more partners and/or for a service/transactional revenue share with one or more partners). In some embodiments, the settlement platform receives and processes (network based) CDRs and/or micro-CDRs. In some embodiments, the settlement platform processes CDRs and/or micro-CDRs for CDR mediation that provides for service usage accounting (e.g., service usage billing allocation and/or service usage/transactional revenue share) on any device activity that is desired. In some embodiments, the settlement platform receives and processes micro-CDRs to determine accounting and settlement information for various services used by such devices. In some embodiments, the settlement platform receives and processes micro-CDRs to determine accounting and settlement information for various services for such devices and distributes the accounting and settlement information to one or more of carriers, distribution partners, MVNOs, wholesale partners, and/or other partners or entities, as described herein.

[0026] In some embodiments, multiple device groups are supported in which each device group is provided an independent and secure management for transparent reconciliation. In some embodiments, a service provider selects who receives a reconciliation report of activations and service usage based on a service plan type. In some embodiments, service usage information (e.g., CDRs and/or micro-CDRs) are used for service plan billing and/or reconciliation reports.

In some embodiments, different service plans on the same device can be communicated to different partners and/or the same partner (e.g., one or more of carriers, distribution partners, MVNOs, and/or wholesale partner). In some embodiments, multi-device and multi-user reconciliation capabilities are provided. In some embodiments, service /transactional revenue share techniques as described herein are provided to augment and/or replace bounty-plus-subsidy models for non-carrier channels. For example, the settlement platform can be used to implement a revenue share model allocating shared service usage revenue among two or more partners (e.g., one or more of carriers, distribution partners, MVNOs, wholesale partners, and/or other partners) for one or more services (e.g., for a discounted bounty or in lieu of a bounty, the mobile device provider can receive a service/transactional revenue share for one or more services provided by a service provider for a mobile device distributed/sold through the service provider).

[0027] **Figure 1** illustrates a wireless network architecture for providing device group partitions and a settlement platform in accordance with some embodiments. As shown, Figure 1 includes a 4G/3G/2G wireless network operated by, for example, a central provider. As shown, various wireless devices 100 are in communication with base stations 125 for wireless network communication with the wireless network (e.g., via a firewall 124), and other devices 100 are in communication with Wi-Fi Access Points (APs) or Mesh 702 for wireless communication to Wi-Fi Access CPE 704 in communication with central provider access network 109. In some embodiments, each of the wireless devices 100 includes a service processor 115 (as shown) (e.g., executed on a processor of the wireless device 100), and each service processor connects through a secure control plane link to a service controller 122 (e.g., using encrypted communications).

[0028] In some embodiments, service usage information includes network based service usage information (e.g., network based service usage measures or CDRs, which can, for example, be generated by service usage measurement apparatus in the network equipment), which is obtained from one or more network elements (e.g., BTS/BSCs 125, RAN Gateways (not shown), Transport Gateways (not shown), Mobile Wireless Center/HLRs 132, AAA 121, Service Usage History/CDR Aggregation, Mediation, Feed 118, or other network equipment). In some embodiments, service usage information includes micro-CDRs. In some embodiments, micro-CDRs are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired. In some embodiments, each device activity that is desired

to be associated with a billing event is assigned a micro-CDR transaction code, and the service processor 115 is programmed to account for that activity associated with that transaction code. In some embodiments, the service processor 115 periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, the service controller 122 or some other network element. In some embodiments, the service controller 122 reformats the heartbeat micro-CDR usage information into a valid CDR format (e.g., a CDR format that is used and can be processed by an SGSN or GGSN or other network elements/equipment used/authorized for generating or processing CDRs) and then transmits it to a network element/function for CDR mediation (e.g., CDR Storage, Aggregation, Mediation, Feed 118).

[0029] In some embodiments, CDR mediation is used to account for the micro-CDR service usage information by depositing it into an appropriate service usage account and deducting it from the user device bulk service usage account. For example, this technique provides for a flexible service usage billing solution that uses pre-existing solutions, infrastructures, and/or techniques for CDR mediation and billing. For example, the billing system (e.g., billing system 123 or billing interface 127) processes the mediated CDR feed from CDR mediation, applies the appropriate account billing codes to the aggregated micro-CDR information that was generated by the device, and then generates billing events in a manner that does not require changes to the existing billing systems (e.g., using new transaction codes to label the new device assisted billing capabilities). In some embodiments, network provisioning system 160 provisions various network elements/functions for authorization in the network, such as to authorize certain network elements/functions (e.g., CDR storage, aggregation, mediation, feed 118 or other network elements/functions) for providing micro-CDRs, reformatted micro-CDRs, and/or aggregated or reconciled CDRs.

[0030] As shown in Figure 1, a CDR storage, aggregation, mediation, feed 118 is provided. In some embodiments, the CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100. In some embodiments, the CDR storage, aggregation, mediation, feed 118 also provides a settlement platform using the mediated micro-CDRs, as described herein. In some embodiments, another

network element provides the settlement platform using aggregated and/or mediated micro-CDRs (e.g., central billing interface 127 and/or another network element/function).

[0031] In some embodiments, various techniques for partitioning of device groups are used for partitioning the mobile devices 100 (e.g., allocating a subset of mobile devices 100 for a distributor, an OEM, a MVNO, and/or another partner or entity). As shown in Figure 1, a MVNO core network 210 includes a MVNO CDR storage, aggregation, mediation, feed 118, a MVNO billing interface 122, and a MVNO billing system 123 (and other network elements as shown in Figure 1). In some embodiments, the MVNO CDR storage, aggregation, mediation, feed 118 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100 (e.g., MVNO group partitioned devices).

[0032] Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing device group partitions and a settlement platform, and Figure 1 is illustrative of just one such example network architecture for which device group partitions and settlement platform techniques described herein can be provided.

[0033] In some embodiments, CDR storage, aggregation, mediation, feed 118 (e.g., service usage 118, including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment apparatus/systems attached to one or more of the sub-networks shown in Figure 1 (e.g., central provider access network 109 and/or central provider core network 110), which is in communication with the service controller 122 and a central billing interface 127. As shown in Figure 1, service usage 118 provides a function in communication with the central provider core network 110. In some embodiments, the CDR storage, aggregation, mediation, feed 118 function is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in the AAA server 121 and/or the mobile wireless center/Home Location Register(HLR) 132 (as shown, in communication with a DNS/DHCP server 126). In some embodiments, service usage 118 functionality is located or partially located in the base station, base station controller and/or base

station aggregator, collectively referred to as base station 125 in Figure 1. In some embodiments, CDR storage, aggregation, mediation, feed 118 functionality is located or partially located in a networking component in the central provider access network 109, a networking component in the core network 110, the central billing system 123, the central billing interface 127, and/or in another network component or function. This discussion on the possible locations for the network based and device based service usage information collection, aggregation, mediation, and reporting function (e.g., CDR storage, aggregation, mediation, feed 118) can be easily generalized as described herein and as shown in the other figures and embodiments described herein by one of ordinary skill in the art. Also as shown in Figure 1, the service controller 122 is in communication with the central billing interface 123 (also sometimes referred to as the external billing management interface or billing communication interface) 127, which is in communication with the central billing system 123. As shown in Figure 1, an order management 180 and subscriber management 182 are also in communication with the central provider core network 110 for facilitating order and subscriber management of services for the devices 100 in accordance with some embodiments.

[0034] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) collects device generated/assisted service usage information (e.g., micro-CDRs) for one or more devices on the wireless network (e.g., devices 100); and provides the device generated service usage information in a syntax and a communication protocol that can be used by the wireless network to augment or replace network generated usage information for the one or more devices on the wireless network. In some embodiments, the syntax is a charging data record (CDR), and the communication protocol is selected from one or more of the following: 3GPP, 3GPP2, or other communication protocols. In some embodiments, as described herein, the CDR storage, aggregation, mediation, feed 118 collects/receives micro-CDRs for one or more devices on the wireless network (e.g., devices 100). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) includes a service usage data store (e.g., a billing aggregator) and a rules engine for aggregating the collected device generated service

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

[0035] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates a new set of CDRs (e.g., aggregated and mediated CDRs and/or micro-CDRs that are then translated into standard CDRs for a given wireless network) for the one or more devices on the wireless network to a billing interface (e.g., central billing interface 127) or a billing system (e.g., central billing system 123). In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller (e.g., service controller 122) to collect the device generated service usage information (e.g., micro-CDRs) for the one or more devices on the wireless network. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a service controller, in which the service controller is in communication with a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates the device generated service usage information to a billing interface or a billing system. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) communicates with a transport gateway and/or a Radio Access Network (RAN) gateway to collect the network generated/based service usage information for the one or more devices on the wireless network. In some embodiments, the service controller 122 communicates the device assisted service usage information (e.g., micro-CDRs) to the CDR

storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements).

[0036] In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs rules for performing a bill by account aggregation and mediation function. In some embodiments, the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs rules for performing a service billing function, as described herein, and/or for performing a service/transactional revenue sharing function, as described herein. In some embodiments, the service controller 122 in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device assisted service usage information (e.g., micro-CDRs). In some embodiments, a rules engine device in communication with the CDR storage, aggregation, mediation, feed 118 (and/or other network elements or combinations of network elements) performs a rules engine for aggregating and mediating the device assisted service usage information.

[0037] In some embodiments, the rules engine is included in (e.g., integrated with/part of) the CDR storage, aggregation, mediation, feed 118. In some embodiments, the rules engine and associated functions, as described herein, is a separate function/device. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as described herein, and communicates with the central billing interface 127. In some embodiments, the service controller 122 performs some or all of these rules engine based functions, as described herein, and communicates with the central billing system 123.

[0038] In some embodiments, a settlement platform service is provided. For example, micro-CDRs can be aggregated and mediated to associate service usage for one or more services used by a communications device (e.g., a user of the communications device). A rules engine or another function can determine a revenue share allocation for the service usage for a particular service to determine the settlement for such service usage for the revenue sharing allocation/model and to distribute accounting and settlement information to one or more of

carriers, distribution partners, MVNOs, wholesale partners, and/or other partners or entities. In some embodiments, the service is a transactional service.

[0039] In some embodiments, duplicate CDRs are sent from the network equipment to the billing system 123 that is used for generating service billing. In some embodiments, duplicate CDRs are filtered to send only those CDRs/records for devices controlled by the service controller and/or service processor (e.g., managed devices). For example, this approach can provide for the same level of reporting, lower level of reporting, and/or higher level of reporting as compared to the reporting required by the central billing system 123.

[0040] In some embodiments, a bill-by-account billing offset is provided. For example, bill-by-account billing offset information can be informed to the central billing system 123 by providing a CDR aggregator feed that aggregates the device assisted service usage data feed to provide a new set of CDRs for the managed devices to the central billing interface 127 and/or the central billing system 123. In some embodiments, transaction billing is provided using similar techniques. For example, transaction billing log information can be provided to the central billing interface 127 and/or the central billing system 123.

[0041] In some embodiments, the rules engine (e.g., performed by the service usage 118 or another network element, as described herein) provides a bill-by-account billing offset. For example, device assisted service usage information (e.g., micro-CDRs) includes a transaction type field or transaction code (e.g., indicating a type of service for the associated service usage information). For example, the rules engine can apply a rule or a set of rules based on the identified service associated with the device generated service usage information to determine a bill-by-account billing offset (e.g., a new CDR can be generated to provide the determined bill-by-account billing offset). In some examples, the determined bill-by-account billing offset can be provided as a credit to the user's service usage account (e.g., a new CDR can be generated with a negative offset for the user's service usage account, such as for network chatter service usage, or transactional service usage, or for any other purposes based on one or more rules performed by the rules engine).

[0042] As another example, for a transactional service, a first new CDR can be generated with a negative offset for the user's service usage account for that transactional service related

usage, and a second new CDR can be generated with a positive service usage value to charge that same service usage to the transactional service provider (e.g., Amazon, eBay, or another transactional service provider). In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127. In some embodiments, the service controller 122 generates these two new CDRs, and the service usage 118 stores, aggregates, and communicates these two new CDRs to the central billing interface 127, in which the central billing interface 127 applies rules (e.g., performs the rules engine for determining the bill-by-account billing offset).

[0043] In some embodiments, the service controller 122 sends the device generated CDRs to the rules engine (e.g., a service usage data store and rules engine, such as CDR storage, aggregation, mediation, feed 118), and the rules engine applies one or more rules, such as those described herein and/or any other billing/service usage related rules as would be apparent to one of ordinary skill in the art. In some embodiments, the service controller 122 generates CDRs similar to other network elements, and the rules (e.g., bill-by-account) are performed in the central billing interface 127. For example, for the service controller 122 to generate CDRs similar to other network elements, in some embodiments, the service controller 122 is provisioned on the wireless network (e.g., by network provision system 160) and behaves substantially similar to other CDR generators on the network).

[0044] In some embodiments, the service controller 122 is provisioned as a new type of networking function that is recognized as a valid, authorized, and secure source for CDRs by the other necessary elements in the network (e.g., CDR storage, aggregation, mediation, feed 118). In some embodiments, if the necessary network apparatus only recognize CDRs from certain types of networking equipment (e.g. a RAN gateway or transport gateway), then the service controller 122 provides authentication credentials to the other networking equipment that indicate that it is one of the approved types of equipment for providing CDRs. In some embodiments, the link between the service controller 122 and the necessary CDR aggregation and mediation equipment is secured, authenticated, encrypted, and/or signed.

[0045] In some embodiments, the CDR storage, aggregation, mediation, feed 118 discards the network based service usage information (e.g., network based CDRs) received from one or more network elements. In these embodiments, the service controller 122 provides the device assisted service usage information (e.g., device based CDRs or micro-CDRs) to the CDR storage, aggregation, mediation, feed 118 (e.g., the CDR storage, aggregation, mediation, feed 118 can just provide a store, aggregate, and communication function(s), as it is not required to mediate network based CDRs and device assisted CDRs), and the device based service usage information is provided to the central billing interface 127 or the central billing system 123.

[0046] In some embodiments, the device based CDRs (e.g., micro-CDRs) and/or new CDRs generated based on execution of a rules engine as described herein are provided only for devices that are managed and/or based on device group, service plan, or any other criteria, categorization, and/or grouping, such as based on ambient service or ambient service provider or transactional service or transactional service provider.

[0047] **Figure 2** illustrates another wireless network architecture for providing device group partitions and a settlement platform in accordance with some embodiments. As shown, Figure 2 includes various devices 100 including service processors 115. For example, devices 100 can include various types of mobile devices, such as phones, PDAs, computing devices, laptops, netbooks, tablets, cameras, music/media players, GPS devices, networked appliances, and any other networked device; and/or devices 100 can include various types of intermediate networking devices, as described herein. The devices 100 are in communication with service control 210 and central provider access and core networks 220. Service policies and accounting functions 230 are also provided in communication with the central provider access and core networks 220. For example, devices 100 can communicate via the central provider access and core networks 220 to the Internet 120 for access to various Internet sites/services (e.g., Google sites/services, Yahoo sites/services, Blackberry services, Apple iTunes and AppStore, Amazon.com, FaceBook, and/or any other Internet service or other network facilitated service).

[0048] In some embodiments, Figure 2 provides a wireless network architecture that supports partitioned device groups, in which each device group can be provided independent and secure management of transparent reconciliation. Those of ordinary skill in the art will

appreciate that various other network architectures can be used for providing device group partitions and a settlement platform, and Figure 2 is illustrative of just another such example network architecture for which device group partitions and settlement platform techniques described herein can be provided.

[0049] In some embodiments, a service provider selects who receives a reconciliation report of activations and usage by service plan type. In some embodiments, service usage information (e.g., based on CDRs and/or micro-CDRs or other service usage measures) are used for service plan billing and for reconciliation reports. In some embodiments, different service plans on the same device (e.g., device 100) can be sent to different partners or the same partner. In some embodiments, multi-device and multi-user reconciliation capabilities are provided. In some embodiments, a settlement platform service is provided. In some embodiments, various revenue share techniques as described herein are provided (e.g., implemented using a settlement platform service, using, for example, service policies and accounting functions 230).

[0050] In some embodiments, partitioned device groups are provided. In some embodiments, each partitioned group of devices (e.g., mobile devices 100) can be uniquely managed with secure admin log-ins. In some embodiments, multi-device, multi-user accounting is provided. In some embodiments, capabilities are provided to support multi-party/multi-service reconciliation records to carriers and carrier partners, which can also support various service/transactional revenue share techniques (e.g., for reducing or eliminating the up-front subsidy and associated up-front subsidy risk of certain bounty models). In some embodiments, service usage and profitability analytics are provided (e.g., using aggregated CDRs/micro-CDRs and service policies and accounting functions 230). For example, a partitioned beta test group of devices can be tested and optimized for various service usage policies and/or service plans, and then the optimized service usage policies and/or service plans can be published to an entire or larger device group. In some embodiments, a carrier can be provided a carrier branded device group, and/or a MVNO can be provided a MVNO branded device group.

[0051] **Figure 3** illustrates a wireless network architecture including a settlement platform in accordance with some embodiments. As shown in Figure 3, a settlement platform 310 is provided (and other network elements are also provided as similarly shown in and

described above with respect to Figure 2). In some embodiments, the settlement platform 310 receives, stores, aggregates and mediates micro-CDRs received from mobile devices 100. In some embodiments, the settlement platform 310 provides a settlement platform using the mediated micro-CDRs, as described herein. In some embodiments, the settlement platform 310 in combination with one or more other network elements/functions provides the settlement platform using aggregated and/or mediated micro-CDRs (e.g., central billing interface 127 and/or service policies and accounting 230). Those of ordinary skill in the art will appreciate that various other network architectures can be used for providing device group partitions and a settlement platform, and Figure 3 is illustrative of just one such example network architecture for which device group partitions and settlement platform techniques described herein can be provided.

[0052] As shown in Figure 3, the settlement platform 310 provides a function in communication with the central provider access and core networks 220. In some embodiments, the settlement platform 310 (e.g., including a billing aggregation data store and rules engine) is a functional descriptor for, in some embodiments, a device/network level service usage information collection, aggregation, mediation, and reporting function located in one or more of the networking equipment apparatus/systems attached to one or more of the sub-networks, which is in communication with the service control 210 and/or service policies and accounting 230. In some embodiments, the settlement platform 310 function is located elsewhere in the network or partially located in elsewhere or integrated with/as part of other network elements (e.g., settlement platform 310 functionality can be located or partially located in the service control 210 and/or the service policies and accounting function 230 as shown in Figure 2; and/or in the AAA server 121, the mobile wireless center/Home Location Register(HLR) 132, the base station 125, the networking component in the central provider access network 109, a networking component in the core network 110, the central billing system 123, the central billing interface 127, and/or in another network component or function, as shown in Figure 1).

[0053] In some embodiments, the settlement platform 310 includes the CDR storage, aggregation, mediation, feed 118 function as shown in and described above with respect to Figure 1 and further provides a device/network level service usage information collection, aggregation, mediation, and reporting function. In some embodiments, the rules engine is

included in (e.g., integrated with/part of) the settlement platform 310. In some embodiments, the rules engine and associated functions, as described herein, is a separate function/device. In some embodiments, the service control 210 performs some or all of these rules engine based functions, as discussed herein, and communicates with the settlement platform 310 and/or the service policies and accounting 230. In some embodiments, the service control 210 includes the service controller 122 as shown in and similarly described above with respect to Figure 1.

[0054] In some embodiments, a settlement platform service is provided at least in part by the settlement platform 310. For example, as similarly described above, micro-CDRs can be aggregated and mediated to associate service usage for one or more services used by a user on a device 100. A rules engine or another function can determine a revenue share allocation for the service usage for a particular service to determine the settlement (e.g., billing and/or revenue share) for such service usage, such as for a service/transactional revenue share, and to distribute accounting and settlement information to one or more of carriers, distribution partners, MVNOs, wholesale partners, and/or other partners or entities. In some embodiments, the service is a transactional service.

[0055] **Figure 4** illustrates a flow diagram for providing device assisted service usage information in accordance with some embodiments. At 402, the process for providing device assisted service usage information begins. At 404, service usage on the device is monitored (e.g., using a service processor executing on a processor of the device). At 406, the monitored service usage is associated with a transaction ID or transaction code (e.g., using a service processor, such as service processor 115 that provides, for example, application service level monitoring, different transaction codes are assigned to Google services, eBay services, Amazon services, Apple iTunes services, and/or other service usage activities/services). In some embodiments, monitored services include transaction based services that are monitored and assigned unique transaction codes. At 408, micro-CDR(s) are generated for the monitored service usage. At 410, the generated micro-CDRs are stored (e.g., at least until the micro-CDR(s) are communicated to the network, such as the service controller or another network element/function, such as service control 210). At 412, a heartbeat communication event is determined. At 414, if a heartbeat communication is to be provided (e.g., to communicate to the network, such as service controller 122 or another network element, such as service control 210),

then the micro-CDRs are sent to the service controller (e.g., service controller 122 or another network element, such as in service control 210). At 416, a request for service usage information is determined. At 418, in response to such a request, the micro-CDRs (e.g., stored or queued micro-CDRs or a set of specifically requested micro-CDRs) are sent to the service controller (e.g., service controller 122 or another network element, such as service control 210). At 420, the process is repeated for any other monitored service usage. At 422, the process is completed.

[0056] **Figure 5** illustrates a flow diagram for providing a settlement platform service in accordance with some embodiments. At 502, the process for a settlement platform begins. At 504, device assisted service usage information is received (e.g., micro-CDRs). At 506, device assisted service usage information is aggregated (e.g., based on the device and the service, such as based on associated settlement platform rules for the device and the service). At 508, the aggregated device assisted service usage information is stored. At 510, the device assisted service usage information is mediated/reconciled (e.g., based on various other measures, such as network based service usage information, and/or other metrics/criteria or techniques, such as the various techniques described herein). At 512, whether the device is a member of a device group is determined. At 514, the rules associated with that device's device group are determined. At 516, whether any settlement platform rules apply to that device group and a given service for the stored device service usage information for the device is determined (e.g., service billing and/or service/transactional revenue share related or other related rules). At 518, the settlement platform rules for the associated service usage for that device and the relevant service are applied. In some embodiments, a revenue share for the service usage for a particular service is used to determine the settlement for such service usage based on the revenue sharing allocation/model and is further used to distribute accounting and settlement information to one or more of carriers, distribution partners, MVNOs, wholesale partners, and/or other partners or entities. In some embodiments, service billing is allocated among one or more partners for a service usage. In some embodiments, a transactional revenue share among one or more partners for a transactional service is applied. At 520, the process is repeated for additional settlement platform rules. At 522, the process is completed.

[0057] 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.

[0058] WHAT IS CLAIMED IS:

CLAIMS

1. A system, comprising:
a processor of a network device in communication with a wireless network, wherein the processor is configured to:
5 collect device generated service usage information for one or more devices in wireless communication on the wireless network; and
aggregate the device generated service usage information for a settlement platform for the one or more devices in wireless communication on the wireless network;
and
10 a memory coupled to the processor and configured to provide the processor with instructions.
2. The system recited in claim 1, wherein the settlement platform determines accounting and settlement information for one or more services for the one or more devices assigned to a
15 device group partition and distributes the accounting and settlement information to one or more of the following associated with the device group partition: a carrier, a distribution partner, an MVNO, and a wholesale partner.
3. The system recited in claim 1, wherein the device generated service usage information is
20 translated into a syntax and a communication protocol that can be used by other network devices to augment or replace network generated service usage information for the one or more devices in wireless communication on the wireless network.
4. The system recited in claim 1, wherein the device generated service usage information
25 includes micro-CDRs.
5. The system recited in claim 1, wherein the device generated service usage information includes micro-CDRs collected by a service controller from a service processor executed on each of the one or more devices in wireless communication on the wireless network.

6. The system recited in claim 1, wherein the device generated service usage information includes micro-CDRs, and wherein at least a subset of micro-CDRs include a transaction code for associating a monitored service usage with a service usage activity.

5

7. The system recited in claim 1, wherein the device generated service usage information is translated into a syntax and a communication protocol that can be used by other network devices to augment or replace network generated service usage information for the one or more devices in wireless communication on the wireless network, wherein the syntax is a charging data record (CDR), and wherein the device generated service usage information includes micro-CDRs.

10

8. The system recited in claim 1, wherein the network device includes a service usage data store.

9. The system recited in claim 1, wherein the network device includes a service usage data store that aggregates and mediates micro-CDRs and network generated CDRs for the one or more devices in wireless communication on the wireless network.

15

10. The system recited in claim 1, wherein the network device includes a service usage data store and a rules engine for aggregating and mediating the collected device generated service usage information.

20

11. The system recited in claim 1, wherein the processor is further configured to:

collect network generated service usage information for the one or more devices in wireless communication on the wireless network.

25

12. The system recited in claim 1, wherein the device generated service usage information is received in a charging data record (CDR) syntax, wherein the device generated service usage information includes micro-CDRs, and wherein the processor is further configured to:

aggregate micro-CDRs for the one or more devices in wireless communication on the wireless network; and

apply a set of rules to the aggregated micro-CDRs using a rules engine to provide aggregated and mediated micro-CDRs to the settlement platform, wherein the settlement platform implements a service billing allocation and/or a revenue share among one or more partners, and wherein the revenue share includes a service based revenue share or a transactional based revenue share.

13. The system recited in claim 1, wherein the device generated service usage information is received in a charging data record (CDR) syntax, wherein the device generated service usage information includes micro-CDRs, wherein the network device includes a CDR storage, aggregation, and mediation feed, and wherein the processor is further configured to:

aggregate micro-CDRs for the one or more devices in wireless communication on the wireless network;

apply a set of settlement platform rules to the aggregated micro-CDRs using a rules engine to generate a new set of CDRs for the one or more devices in wireless communication on the wireless network; and

communicate the new set of CDRs for the one or more devices in wireless communication on the wireless network to a billing interface or a billing system.

20

14. The system recited in claim 1, wherein the device generated service usage information is received in a charging data record (CDR) syntax, wherein the device generated service usage information includes micro-CDRs, and wherein the processor is further configured to:

aggregate micro-CDRs for the one or more devices in wireless communication on the wireless network;

25

verify at least a subset of the micro-CDRs;

apply a set of settlement platform rules to the aggregated and verified micro-CDRs using a rules engine to generate a new set of CDRs for the one or more devices in wireless communication on the wireless network; and

communicate the new set of CDRs for the one or more devices in wireless communication on the wireless network to a billing interface or a billing system.

15. The system recited in claim 1, wherein the device generated service usage information is received in a charging data record (CDR) syntax, wherein the device generated service usage information includes micro-CDRs, and wherein the processor is further configured to:

aggregate micro-CDRs for the one or more devices in wireless communication on the wireless network;

verify the micro-CDRs by comparing at least a subset of the micro-CDRs to a set of network generated CDRs for the one or more devices in wireless communication on the wireless network;

apply a set of settlement platform rules to the aggregated and verified micro-CDRs using a rules engine to generate a new set of CDRs for the one or more devices in wireless communication on the wireless network; and

communicate the new set of CDRs for the one or more devices in wireless communication on the wireless network to a billing interface or a billing system.

16. The system recited in claim 1, wherein the device generated service usage information is received in a charging data record (CDR) syntax, wherein the device generated service usage information includes micro-CDRs, and wherein the processor is further configured to:

aggregate the micro-CDRs for the one or more devices in wireless communication on the wireless network;

apply a set of rules to the aggregated micro-CDRs using a rules engine to generate a new set of CDRs, wherein the set of rules includes a bill by account rule; and

communicate the new set of CDRs for the one or more devices in wireless communication on the wireless network to a billing interface or a billing system.

17. The system recited in claim 1, wherein the device generated service usage information is received in a charging data record (CDR) syntax, wherein the device generated service usage information includes micro-CDRs, and wherein the processor is further configured to:

aggregate the micro-CDRs for the one or more devices in wireless communication on the wireless network;

apply a set of rules to the aggregated micro-CDRs using a rules engine to generate a new set of CDRs, wherein the set of rules includes a bill by account rule; and

5 communicate the new set of CDRs for the one or more devices in wireless communication on the wireless network to a billing interface or a billing system, wherein at least one CDR in the new set of CDRs includes a billing offset.

18. The system recited in claim 1, wherein the device generated service usage information is
10 received in a charging data record (CDR) syntax, wherein the device generated service usage information includes micro-CDRs, and wherein the processor is further configured to:

 communicate a new set of CDRs based at least in part on aggregated micro-CDRs for the one or more devices in wireless communication on the wireless network to the settlement platform, wherein the settlement platform determines accounting and settlement information for
15 one or more services for the one or more devices assigned to a device group partition and distributes the accounting and settlement information to one or more of the following associated with the device group partition: a carrier, a distribution partner, an MVNO, and a wholesale partner.

20 19. The system recited in claim 1, wherein the processor is further configured to:
 store the aggregated device generated service usage information; and
 implement a settlement platform to mediate the device generated service usage information.

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

store the aggregated device generated service usage information; and
apply a set of settlement platform rules to mediate the device generated service usage information, wherein the set of settlement platform rules are selected based at least in part on a device group partition determination for each of the one or more devices.

5

21. The system recited in claim 1, wherein the processor is further configured to:
store the aggregated device generated service usage information;
apply a set of settlement platform rules to mediate the device generated service usage information, wherein the set of settlement platform rules are selected based at least in part on a
10 device group partition determination for each of the one or more devices; and
communicate a new set of CDRs to a billing interface based at least in part on the mediated device generated service usage information.

22. The system recited in claim 1, wherein the processor is further configured to:
15 communicate the device generated service usage information to a billing interface,
wherein the billing interface includes a settlement platform.

23. The system recited in claim 1, wherein the processor is further configured to:
collect the device generated service usage information for the one or more devices in
20 wireless communication on the wireless network from an intermediate networking device,
wherein the device generated service usage information includes a transaction code for associating a user of a first device, the first device, and/or the intermediate networking device with the device generated service usage information, wherein the one or more devices includes the first device.

25

24. A method, comprising:
collecting device generated service usage information for one or more devices in wireless communication on a wireless network; and

aggregating the device generated service usage information for a settlement platform for the one or more devices in wireless communication on the wireless network.

25. A computer program product, the computer program product being embodied in a
5 computer readable storage medium and comprising computer instructions for:
- collecting device generated service usage information for one or more devices in wireless communication on a wireless network; and
 - aggregating the device generated service usage information for a settlement platform for the one or more devices in wireless communication on the wireless network.

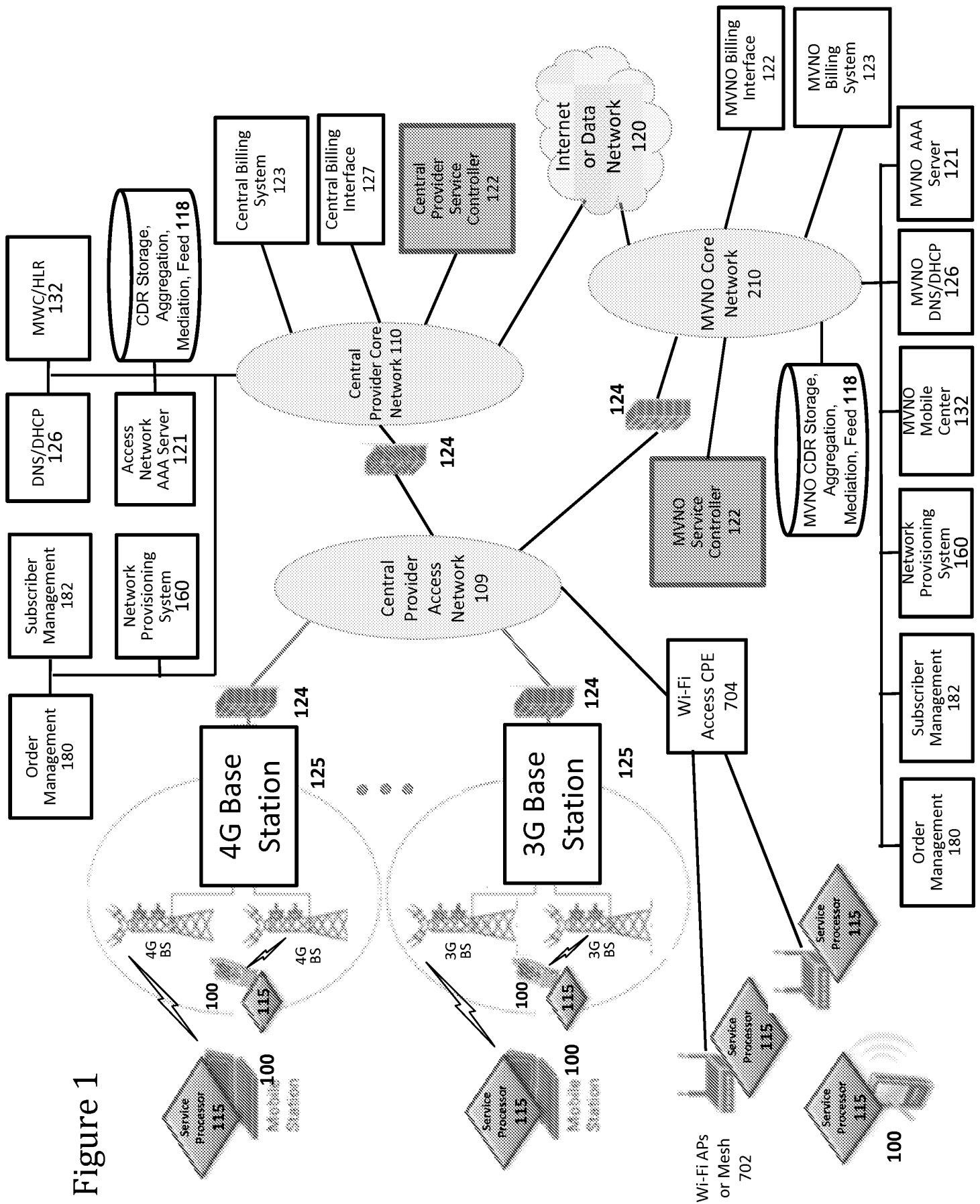
10

DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM

ABSTRACT OF THE DISCLOSURE

[0059] Device group partitions and a settlement platform are provided. In some embodiments, device group partitions (e.g., partitions of devices based on associated device groups) are provided. In some embodiments, a settlement platform service is provided. In some embodiments, a settlement platform service is provided for partitioned devices. In some embodiments, collecting device generated service usage information for one or more devices in wireless communication on a wireless network; and aggregating the device generated service usage information for a settlement platform for the one or more devices in wireless communication on the wireless network is provided. In some embodiments, a settlement platform implements a service billing allocation and/or a service/transactional revenue share among one or more partners. In some embodiments, service usage information includes micro-CDRs, which are used for CDR mediation or reconciliation that provides for service usage accounting on any device activity that is desired. In some embodiments, each device activity that is desired to be associated with a billing event is assigned a micro-CDR transaction code, and a service processor of the device is programmed to account for that activity associated with that transaction code. In some embodiments, a service processor executing on a wireless communications device periodically reports (e.g., during each heartbeat or based on any other periodic, push, and/or pull communication technique(s)) micro-CDR usage measures to, for example, a service controller or some other network element for CDR mediation or reconciliation.

Figure 1



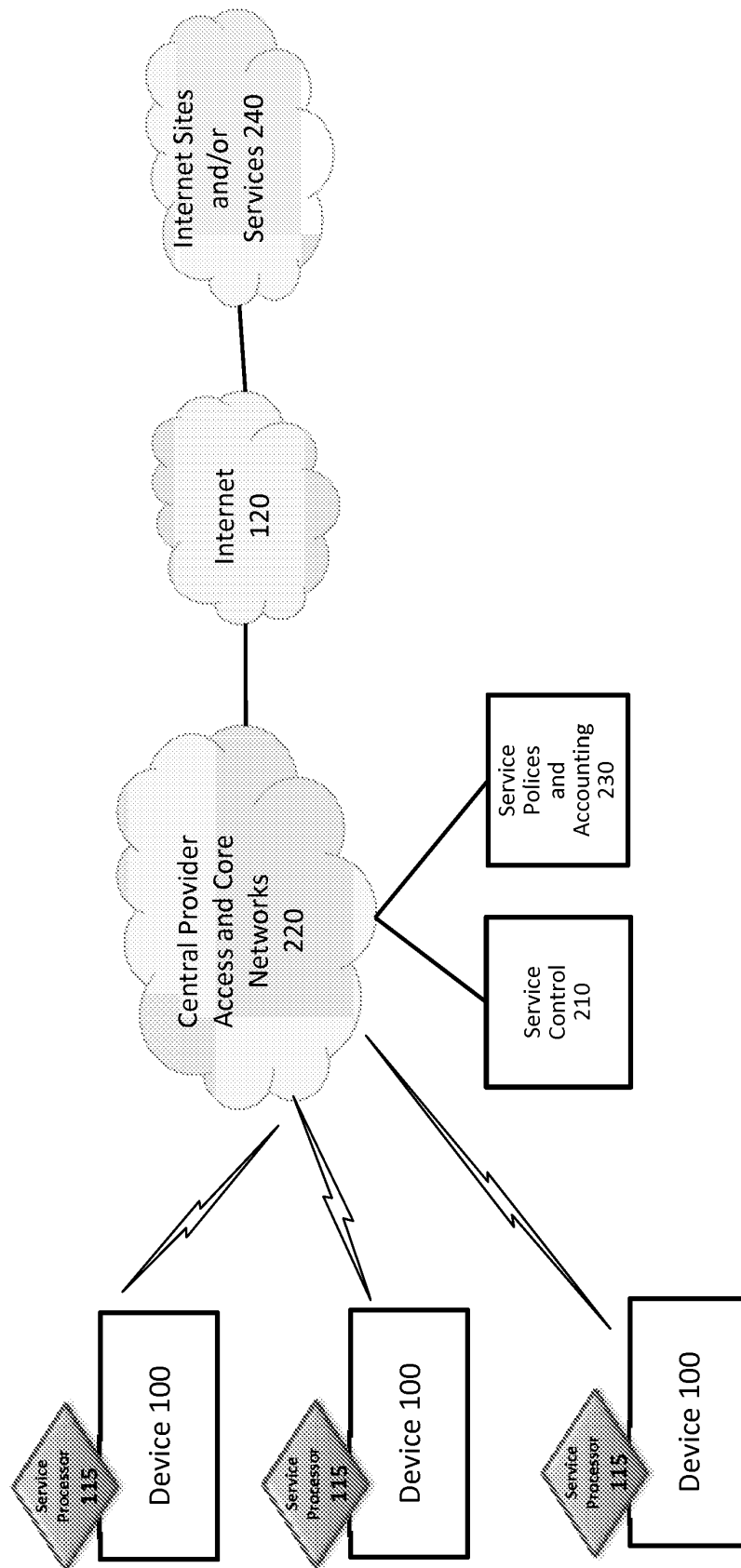


Figure 2

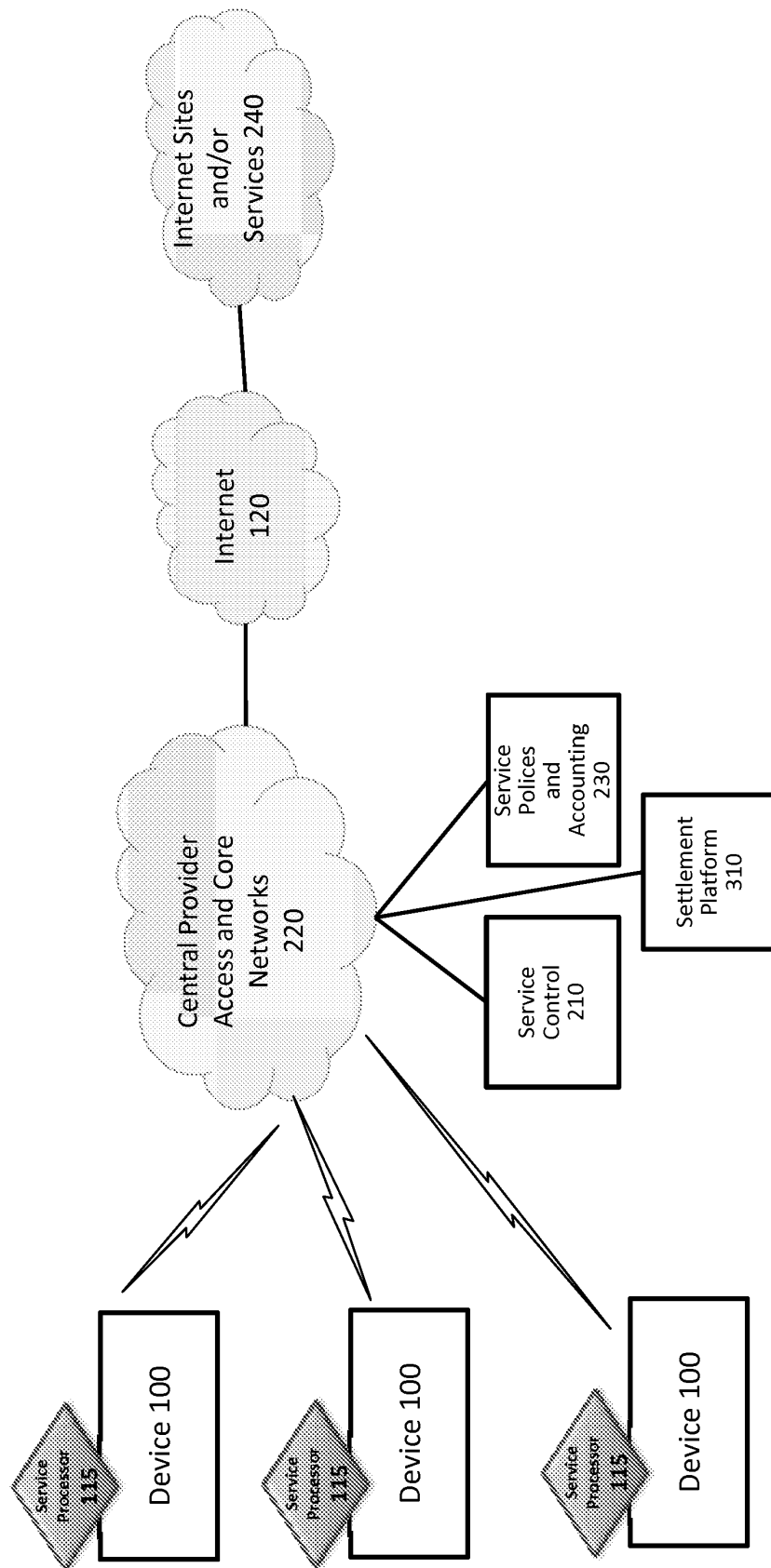


Figure 3

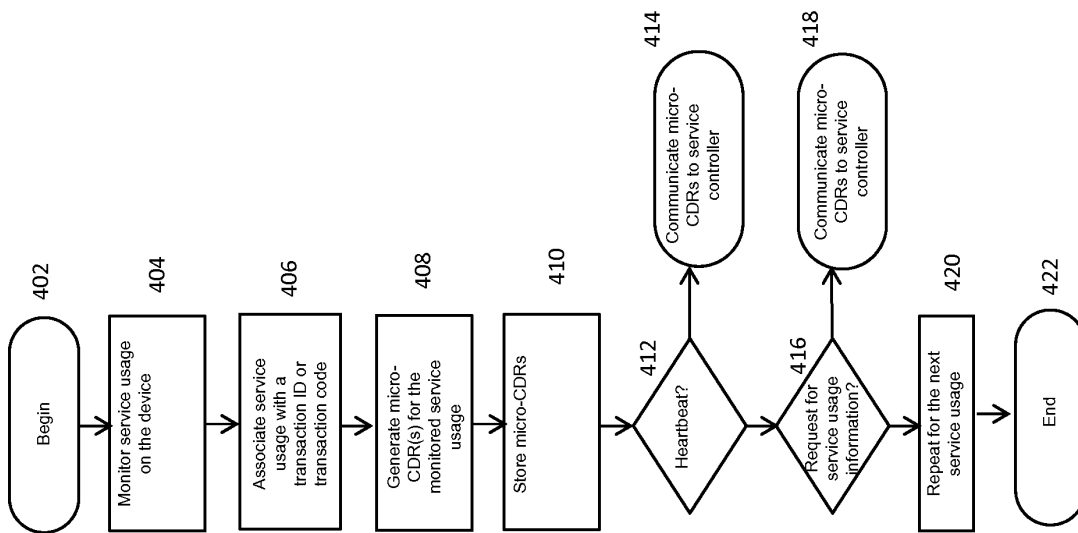


Figure 4

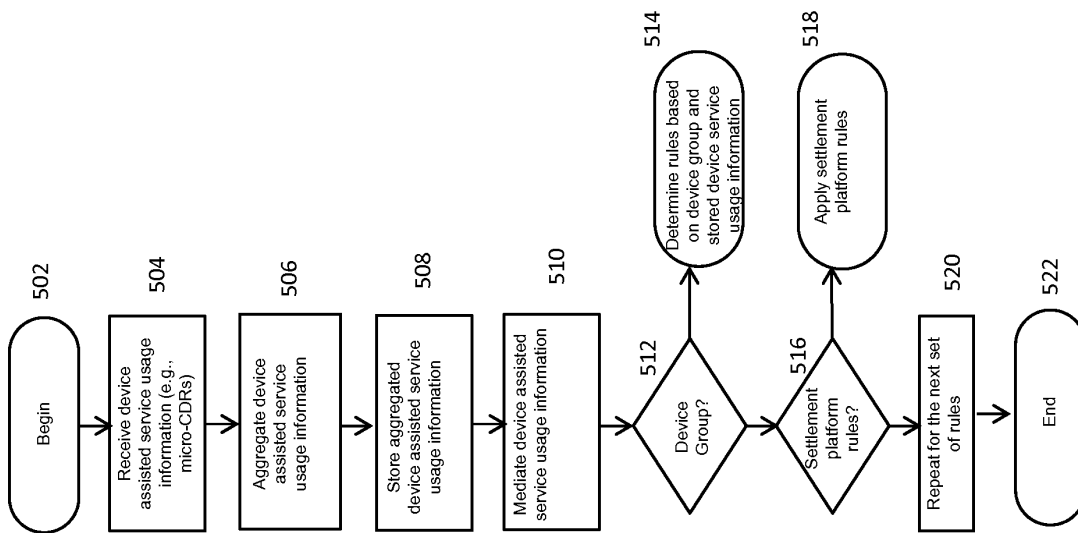


Figure 5

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	RALEP026
		Application Number	
Title of Invention	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM		
<p>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.</p>			

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	Countryi				
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	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM		
Attorney Docket Number	RALEP026	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)	5	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP026
		Application Number	
Title of Invention	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM		

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	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	RALEP026
		Application Number	
Title of Invention	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61270353	2009-07-06
Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61252153	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

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	RALEP026
		Application Number	
Title of Invention	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM		

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.

Electronic Acknowledgement Receipt	
EFS ID:	6885920
Application Number:	12694451
International Application Number:	
Confirmation Number:	6041
Title of Invention:	DEVICE GROUP PARTITIONS AND SETTLEMENT PLATFORM
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:	RALEP026
Receipt Date:	27-JAN-2010
Filing Date:	
Time Stamp:	12:56:06
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		RALEP026_APP.pdf	164454	yes	35
			0aafb7bf461e776f4b58b5024577329acaf5df5f		

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal of New Application		1	1	
	Specification		2	27	
	Claims		28	34	
	Abstract		35	35	
Warnings:					
Information:					
2	Drawings-only black and white line drawings	RALEP026_Figures.pdf	672288	no	5
			2f372ffbabe618358bd2afd6c5d85be5b37c4d50		
Warnings:					
Information:					
3	Application Data Sheet	RALEP026_Application_Data_Sheet_sb0014_fill.pdf	967953	no	5
			c12b72266369147ac47b2443f61b33a1a729c742		
Warnings:					
Information:					
Total Files Size (in bytes):			1804695		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					

SCORE Placeholder Sheet for IFW Content

Application Number: 12694451

Document Date: 1/27/2010

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (<http://es/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006

Date: 01/27/10

PTO/SB/06 (12-04)

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 12/694,451	
APPLICATION AS FILED – PART I						
(Column 1)		(Column 2)		SMALL ENTITY		OR
OTHER THAN SMALL ENTITY						
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	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), (l), 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		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)		(Column 2)		(Column 3)		SMALL ENTITY
OTHER THAN SMALL ENTITY						OR
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)
Total (37 CFR 1.16(i))	*	Minus **	=	X =		X =
Independent (37 CFR 1.16(h))	*	Minus ***	=	X =		X =
Application Size Fee (37 CFR 1.16(s))						
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))				N/A		N/A
				TOTAL		TOTAL
				ADD'T FEE		ADD'T FEE
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY
OTHER THAN SMALL ENTITY						OR
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)
Total (37 CFR 1.16(i))	*	Minus **	=	X =		X =
Independent (37 CFR 1.16(h))	*	Minus ***	=	X =		X =
Application Size Fee (37 CFR 1.16(s))						
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))				N/A		N/A
				TOTAL		TOTAL
				ADD'T FEE		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.