EUROPEAN PATENT SPECIFICATION

Date of publication and mention of the grant of the patent:
03.04.2019 Bulletin 2019/14

Application number: 16171788.9

Date of filing: 27.05.2016

METHODOLOGY AND APPARATUS FOR DYNAMIC CELLULAR NETWORKING ACTIVATION FOR
VIRTUAL SIM SERVICE

METHOD AND APPARATUS FOR DYNAMIC CELLULAR NETWORKING ACTIVATION FOR
VIRTUAL SIM SERVICE

VERFAHREN UND VORRICHTUNG ZUR AKTIVIERUNG DER DYNAMISCHEN ZELLULAREN
VERNETZUNG FÜR VIRTUELLEN SIM-DIENST

PROCÉDÉ ET APPAREIL POUR L'ACTIVATION D'UNE MISE EN RÉSEAU CELLULAIRE
DYNAMIQUE DE SERVICES SUR CARTE SIM VIRTUELLE

Designated Contracting States:
AL AT BE BG CY CZ DE DK EE ES FI FR GB HR HU IE IS IT LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Priority: 29.05.2015 US 201514725450

Date of publication of application:

Proprietors:
• BlackBerry Limited
  Waterloo, ON N2K 0A7 (CA)
• 2236008 Ontario Inc.
  Waterloo, ON N2K 0A7 (CA)

Inventors:
• PIEDA, Peter Steven
  Ottawa, Ontario K1V 2J7 (CA)
• NAGARAJAN, Sivakumar
  Ottawa, Ontario K1S 1K1 (CA)

Representative: Hanna Moore + Curley
Garryard House
25/26 Earlsfort Terrace
Dublin 2, D02 PX51 (IE)

References cited:
JP-A- 2011 192 129
US-B2- 8 996 002

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).
Description

FIELD OF THE DISCLOSURE

[0001] The present disclosure relates to mobile devices and in particular relates to mobile devices having both work and personal applications.

BACKGROUND

[0002] The use of user equipment (UE) or mobile devices, including smartphones, cellphones, laptops, digital pagers, among others, is becoming more prevalent. Many of these UEs have at least one cellular connection which may be used for both circuit switch and packet switch calls. Such cellular connections are usually based on a subscription or pre-paid plan with a cellular provider.

[0003] In order to access the cellular provider’s network, a smart card such as a universal integrated circuit card (UICC) is typically found on such devices, where the UICC has one or more applications used for subscriber identity verification. Such applications may, for example, include a subscriber identity module (SIM) application or a universal subscriber identity module (USIM) application for the global system for mobile communication (GSM) networks, for a universal mobile telecommunications system (UMTS) system or long term evolution (LTE) system, a code division multiple access (CDMA) subscriber identity module application (CSIM application) for a CDMA 2000 network, a remote-user identity module (RUIM) for a CDMA network, IP multimedia services (IMS) subscriber identity module (SIM) for IMS services, among others. Once authenticated to the network, the user equipment may then exchange voice or data, depending on the subscription with the cellular network.

[0004] One trend in the workplace is to bring your own device (BYOD) policy for employers, where employees may bring their own device and be connected to enterprise services on that device. However, allocation of resources and billing for such systems is complex, since it is difficult to distinguish between personal and work phone calls, text messages, and data usage and the associated costs and billing between the two. A similar trend exists for corporate owned and personal enabled (COPE) devices, where employees are issued a corporate device that may be connected to personal services and applications.

[0005] US 8996002B2 describes apparatus and methods for provisioning wireless devices for operation in one or more networks. A provisioning service may provide access client (e.g., SIM) data to a secure element in the wireless user device. The device may be preloaded with a provisioning SIM profile. The device may use the provisioning profile to roam onto a carrier, and communicate with a provisioning service, which may present the user with a list of available wireless carriers. In response to a user selection, the provisioning service may load a SIM profile associated with the selected carrier onto the secure element. The loaded SIM profile can be used to obtain wireless service from the selected carrier. The user may add multiple SIM profiles, and/or may delete SIM profiles.

[0006] JP 2011/192129 describes an authentication system including a user terminal, a portable telephone terminal, an authentication server, and a user information management DB. The user terminal includes a means for acquiring IMSI information of the portable telephone terminal connected to the user terminal, and a means for acquiring MAC address information of the user terminal, and a means for transmitting the IMSI and MAC address information to the authentication server and receiving log-in authentication. The authentication server include a means for receiving the IMSI information and the MAC address information of a log-in authentication request from the user terminal, and inquiring whether some information has been registered to the user management information DB to perform log-in authentication.

[0007] EP 2680663 A1 describes a method for routing a communication including receiving, from an application running on a user equipment (UE), a request to access a forwarding information base (FIB). The UE includes a plurality of FIBs and a plurality of communication interfaces. Each of the plurality of FIBs includes communication interface information. An assigned FIB from the plurality of FIBs is determined. The assigned FIB has been assigned to the application. An appropriate communication interface for communication is determined based on a destination of the communication and the communication interface information of the assigned FIB. The communication is transmitted to the destination using the communication interface.

[0008] US 2012/0108204 describes methods and apparatus for managing multiple user access control entities or clients. For example, a "wallet" of electronic subscriber identity modules (eSIMs) may be stored and used at a user device and/or distributed to other devices for use thereon. A networked server may store and distribute eSIMs to a plurality of user devices in communication therewith. A database of available eSIM is maintained at the wallet entity and/or at the network which enables request for a particular eSIM to be processed and various rules for the distribution thereof to be implemented. Security precautions are implemented to protect both user and network carrier specific data as the data is transmitted between networked entities. Solutions for eSIM backup and restoration are also described.

SUMMARY

[0009] Accordingly there is provided a method, computer program and user equipment as detailed in the claims that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The present disclosure will be better under-
The present disclosure provides a method at a user equipment to facilitate activation and splitting of data billing between at least two parties, the method comprising: starting, at the user equipment, a virtual subscriber identity module platform (‘VSP’) service on the user equipment; verifying VSP configuration information with a network server; upon verification, starting a virtual subscriber identity module platform (‘VSP’) service on the UE, a VSP daemon on the UE can start a virtual subscriber identity module platform (‘VSP’) service on the user equipment; verifying VSP configuration information with a network server; upon verification, starting a data networking access point name (‘APN’) based on the configuration information on the user equipment; and setting a status indicator on the user equipment to indicate the VSP service is enabled.

Specifically, the present disclosure relates to the addition of one or more identities on a device to allow split billing between such identities. For example, a work and personal plan can be added to a single device, where work phone calls, text messages and data used for work applications may be billed to an employer, whereas personal phone calls, text messages and data usage may be billed to an individual user of the device. However, the present disclosure is not limited to a work and personal split, and the addition of multiple plans to a device is contemplated by the present disclosure. For example, in another embodiment a device may be split between two users and each user may have a separate plan on the device.

In accordance with one embodiment of the present disclosure, multiple billing plans are implemented utilizing a virtual SIM platform (VSP) at a carrier which allows the user to have multiple phone lines in a single SIM in a phone. As used herein, a SIM can be any identity module. Such split allows a user to have voice and data split billing between the work and personal lines.

In accordance with one embodiment of the present disclosure, one issue for data networking over cellular is that resources may need to be allocated for such data networking. However, if such resources are allocated before the service is enabled or activated on a user equipment, a carrier may have internet protocol (IP) and other resources allocated for a phone in their network without having such corresponding service activated. This will cause the carrier to waste resources for devices who do not have such service allocated.

Thus, in accordance with the embodiments of the present disclosure, the cellular data network for work traffic is not activated until the virtual SIM service has been started and verified with the VSP at the carrier network.

Specifically, when an enterprise activates the VSP service on the UE, a VSP daemon on the UE can start a VSP application. The VSP application may do the registration authentication and if successful, the VSP daemon may then start the data networking access point name (APN) based on configuration information stored within the UE. Upon starting the data networking APN, the UE may then send a system indicator that such APN is configured, allowing the carrier then to accept data over such APN.

Conversely, when the service is disabled, such as when the user leaves the services, then the APN may shut down.

Each of the processes for bring up and taking

Figure 1 is an example communication system using each of multiple forwarding information bases (MFIbs) for different applications;
Figure 2 is an example forwarding information base;
Figure 3 is a block diagram showing a user equipment communicating through a carrier network with either public or enterprise servers;
Figure 4 is a data flow diagram showing initialization of a VSP service on a user equipment;
Figure 5 is a data flow diagram showing activation of a VSP application to create a circuit switched connection;
Figure 6 is a data flow diagram showing configuration of an APN in a persistent object store;
Figure 7 is a data flow diagram showing the activation of a second data access point name (APN);
Figure 8 is a data flow diagram showing the deletion of a VSP service from a device;
Figure 9 is a data flow diagram showing deactivation of a second APN;
Figure 10 is a process diagram showing the steps of activating and deactivating an APN; and
Figure 11 is a block diagram of an example mobile device capable of being used with the embodiments of the present disclosure.
down an APN are described below.

[0021] Reference is now made to Figure 1, which shows an exemplary simplified diagram of a communications system. The communications system includes user equipment 102 communicably coupled to a public network 104 and an enterprise network 106. The UE 102 comprises a network stack 107 including multiple forwarding information bases (FIBs).

[0022] In some implementations, a forwarding information base is a data structure that associates destination with communication interface information. Such communication interface information may for example include a physical interface.

[0023] A UE may have multiple FIBs (MFIBs). In this case, the UE may route communication based on various criteria. For example, different FIBs may be assigned to different applications. In other cases, different FIBs may be used for different prioritization of shared network resources. For example, one FIB may be associated with a trust domain or perimeter for work applications and may give higher priority to certain interfaces within the FIB. In other cases, different FIBs may prioritize networks by type based on a policy decision made external to the UE, such as by a user, corporation, among others.

[0024] In the example of Figure 1, a UE 102 includes two FIBs, namely FIB 108a and FIB 108b. However, this is merely an example and in other cases more FIBs could be included on the device. For example, a device may have a FIB for personal applications, a FIB for work and secure applications, a FIB for tethering, and a FIB for enterprise administration.

[0025] Each FIB is associated with a communication channel (110a and 110b) from applications (112a and 112b).

[0026] Various interfaces, including Wi-Fi 114a, cellular 114b, local area network (LAN) 114c, and Bluetooth™ 114d are shown in UE 102.

[0027] The Network Stack 107 may receive requests to access the FIB 108a, 108b. If access to the requested FIB 108a, 108b is granted, the FIB 108a, 108b may provide routing information to the Application 112a, 112b from which the request originated. In some cases, the Network Stack 107 may merely receive a communication and determine which FIB 108a, 108b is mapped to the Communication Channel 110a, 110b.

[0028] In Figure 1, communication channel 110a routes communication for application 112a based on the routing information provided by FIB 108a, and the communication channel 110b routes communication for application 112b based on the routing information provided by FIB 108b. Applications 112a and 112b may be configured to provide services to one or more users, and each of the physical interfaces 114a-d may communicate with at least one of the public network 104 or the enterprise network 106.

[0029] UE 102 may comprise a tablet, mobile device, personal computer, laptop computer, among others. The embodiment of Figure 1 is however not meant to be limiting and other devices could be used.

[0030] UE 102 generally includes a processor which controls the overall operation of the device. Processor interacts with device subsystems such as for example a display, memory, auxiliary input/output (I/O) subsystems, serial port, one or more keyboards or keypads, where keyboard or keypad may comprise a physical keyboard or a virtual keyboard or both, one or more speakers, microphone, other communication subsystem such as a short-range communications subsystem, including Bluetooth and near field communications, and any other device subsystems. Serial port could include a USB port or other port.

[0031] Memory of UE 102 may be segregated into various modes of operation, sometimes referred to as perimeters, as described below. Such segregation may be physical or logical. Operating system software used by the processor may be stored in such memory. The operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile memory such as random access memory (RAM).

[0032] Applications may be loaded onto the device and associated with a mode of operation (also called a ‘perimeter’) in some cases. In some embodiments, such applications and data for the application may be stored in memory and associated with the perimeter. For example, separate areas of memory may be used to store the applications or data for each perimeter in some embodiments. In other embodiments, applications or data may be encrypted with a key associated with a perimeter and applications or data for a plurality of perimeters may be stored together. Other options are possible.

[0033] In the example of Figure 1, network stack 107 may include any software, hardware, firmware or combination thereof configured to coordinate communication with applications 112a and 112b using the FIBs 108a and 108b and the physical interfaces 114a-d. For example, the network stack 107 may verify whether a requesting application 112a has been granted permissions for access to FIB 108a and, if so, provide the application 112a access to the FIB 108a. In some cases, the network stack 107 may manage FIBs 108a and 108b and manage connection of communication channels 110a and 110b with FIBs 108a and 108b.

[0034] FIBs 108a and 108b may include any parameters, variables, policies, algorithms, instructions, settings or rules for routing communication to at least one of the Public Network 104 or the Enterprise Network 106. For example, the FIB 108a, 108b may map a destination address to a Physical Interface 114a-d, another FIB, another communication channel or others. In general, the FIB 108a, 108b may be any data structure configured to map or otherwise associate a destination address to a Physical Interface 114a-d. However, FIBs 108a, 108b may equally be comprised of any other data structure and still be within the scope of the present disclosure.

[0035] In some cases, FIBs 108a, 108b may include or otherwise identify one or more of the following: desti-
The communication channel 110a, 110b can include any software, hardware, firmware or combination thereof configured to route communication from application 112a, 112b to at least one of the public network 104 or the enterprise network 106. For example, the communication channel 110a, 110b may be an inter-process communication (IPC) channel between the application and the network stack configured to determine a physical interface 114a-d to route communication based on the FIB 108a, 108b.

In some implementations, the communication channel 110a, 110b may be one endpoint of a two-way communication link between an application 112a, 112b and an application running in the public network 104 or the enterprise network 106. For example, the communication channel 110a, 110b may be bound to a port number for a physical interface 114a-d so that the transmission control protocol (TCP) layer can identify the application 112a, 112b to which data is destined to be sent. In some cases, an application 112a, 112b may access the same communication channel 110a, 110b for all communications and the communication channel 110a, 110b may switch between accessing the different FIBs 108a, 108b.

The applications 112a, 112b may be any application, program, module, process or software that may execute, change, delete, generate or otherwise manage information, such as business information, according to the present disclosure. For example, the application 112a, 112b may include a notification application, a contacts application, a calendar application, a messaging application or others. Further, while illustrated as internal to UE 102, one or more processes associated with the application 112a, 112b may be stored, references or executed remotely.

In some cases, applications 112a, 112b may be configured to access different perimeters, such as a personal perimeter or an enterprise perimeter.

In connection with determining an interface 114a-d, the application 112a, 112b may execute one or more of the following: determine a FIB 108a, 108b based on MFIBs assigned to the application 112a, 112b; transmit a request for access to a FIB 108a, 108b to the network stack 107; determine a physical interface 114a-d for the destination based on an assigned FIB 108a, 108b; determine whether an assigned FIB 108a, 108b identifies a further FIB 108a, 108b to use to identify the physical interface 114; determine the physical interface 114 to be used based on the destination of a communication and the further FIB 108a, 108b; or others.

UE 102 may include interfaces 114a-d for communication with other computer systems over at least one of the public network 104 or the enterprise network 106 in a client-server or other distributed environment. In certain implementations, the UE 102 receives data form internal or external senders through interfaces 114a-d for local storage, processing or both.

Generally, interfaces 114a-d comprise logic-encoded in software, hardware, firmware or a combination thereof operable to communicate with at least one of the public network 104 or the enterprise network 106. More specifically, the interfaces 114a-d may comprise software supporting one or more communication protocols associated with the public network 104 or the private or enterprise network 106, or comprise hardware operable to communicate physical signals.

The examples of interfaces 114a-d in Figure 1 are merely illustrative, and other interfaces are possible. The present disclosure is not limited to the particular interfaces shown in the figure.

Reference is now made to Figure 2, which illustrates an example FIB108a. In particular, FIB 108a comprises a routing table which may include a destination column 202, a gateway column 204, flags column 206, refs column 208, use column 210, Mtu column 212 and interface 114. The destination column 202 may identify a destination network address. The gateway 204 may identify an address of the outgoing interface. The flags column 206 may identify a state of the route. The use column 210 may identify a count of the number of packets sent using that route. The Mtu column 212 may identify a maximum transmission unit. The interface 114 may identify a physical interface.

Thus, for example, FIB 108a may map or otherwise associate a destination network address to a physical interface 114. As illustrated in the example of Figure 2, the address "25.48.90.204/30" maps to the "msm0" at the physical interface. In addition to interfaces 114, the FIB 108a may map or associate a destination network address to a different FIB, another communication channel 110, or other elements.

The above device may be used with various networks. Reference is now made to Figure 3, which shows a block diagram of an example wireless data network in accordance with the present disclosure and with which the various embodiments of the methods of the instant disclosure may cooperate.

In the example of Figure 3, UEs 302 are connected over a mobile carrier network 303 for communication through a firewall 305 to a relay 307 within a network operation center 308. A device that receives policies through an enterprise mobility management server, such as a BlackBerry Enterprise Service, may use such infrastructure. As seen in Figure 3, communication from one of UEs 302 is received at relay 307 and passed via a secure channel 309 through firewall 311 to a corporate enterprise server 313 and corporate mobile data system (MDS) server 315.

Similarly, policies and data may be pushed from enterprise server 313 to a UE 302 through firewall 311,
prise servers, such as server 313 and MDS server 315, as well as over carrier network 303 to the internet 320, for example for personal applications.

A module within a network operation center that is carrier controlled is shown in Figure 3 as virtual SIM platform (VSP) 330, which may provide a virtual SIM for a UE 302. In particular, VSP 330 may allow a UE 302 to have a real SIM from the carrier, as well as a virtual SIM. The combination of the real SIM and virtual SIM allow a device 302 to have a plurality of voice and data connections to a cellular network as described below.

Utilizing the above architecture, data billings split can be provided in two ways. A first method is to use a dual access point name (APN) in which there are two APNs provided by a carrier. A carrier may then track how much data is utilized on each APN.

In a second embodiment, counters may be used. In this case, the carrier only has one APN but needs to count on the device how much data is sent via the work or personal spaces. While the counter may be used in certain circumstances, the description below will utilize the dual APN process.

In order to support split billing on a device in accordance with the embodiments described below, the device will need to support a VSP service. Once the VSP service is configured for both voice and data, the network through the carrier may be routed on different interfaces, allowing the carrier to bill the circuit switched or packet switched calls correctly. Specifically, on a VSP device activation, a second data APN can be added along with a work cellular logical interface. Data over the second APN may then be considered work data and billed appropriately.

Reference is now made to Figure 4. In Figure 4, a data flow is shown for enabling the virtual number and data connection for a UE 410. In particular, an enterprise may wish to have both a work and a personal billing enabled on a UE 410. In this case, an enterprise server 412 obtains, from a VSP server 414, a virtual phone number from the VSP. The enterprise server 412 may then send VSP information for a UE 410, including the virtual phone number, as well as other information. Such information may include, for example, an identifier, such as an international mobile subscriber identity (IMSI), that was obtained from UE 410 when a SIM card was inserted.

The enterprise server 412 communicates with an enterprise management agent (EMA) 414 on UE 410. Enterprise server 412 may push the previously obtained VSP information to the enterprise management agent 414, as shown by message 430. In one embodiment, an identifier is also pushed to the UE 410. For example, such identifier may be an international mobile subscriber identity (IMSI) created for the virtual SIM.

The enterprise management agent 414 may receive the message 430 from enterprise server 412 and consider this to be a policy of the enterprise and cause actions to be taken on UE 410. Further, enterprise management agent 414 sends acknowledgement message 432 back to the enterprise server 412.

Enterprise management agent 414 may store the persistent objects found within message 430 on the device for future use. For example, enterprise management agent 414 may store VSP information within its own database or in a persistent object store for the enterprise management agent 414.

The carrier policy manager 416 communicates with a database that may be located on an actual SIM within device 410. Such database is shown with reference 418 in the embodiment of Figure 4. In other embodiments, the database 418 may be located on the device but may be populated when a SIM is inserted into device 410. As part of the carrier’s configuration of UE 410, the carrier policy manager 416 may receive the second APN cellular configuration.

A virtual preload (VPL) of a VSP application may then occur. The virtual preload (VPL) may, in some embodiments, be provided to a user for the user’s approval. In particular, as shown in Figure 4, user 420 will receive message 436 asking whether or not the virtual preload for the VSP service is okay and if the user approves, as shown by message 438, then the procedure for installing the VSP service may continue.

The carrier information manager 416 may then request, from an application server 422, the VSP service application. Such request is shown by message 440. Application server 422 may be any remote server providing application data to a mobile device (i.e UE 410).

The application server 422 returns the VSP service application, as shown by message 442. Message 442 causes the application to be launched and installed on the device.

The launching may involve several processes. For example, VSP service 424 may, once launched, listen to the enterprise management agent 414 to determine whether the VSP information provided by the enterprise server 412 is okay, as shown by block 444. If yes, then the process may proceed to block 450 in which the VSP application is started.

As used herein, a VSP application is the entity that communicates with the VSP network component for virtual SIM information, including the virtual phone number. The VSP service interfaces with the system to give deep integration into the device. Such VSP service includes the user interface components, SMS, the second APN being brought up, among other functionality.

Referring again to Figure 4, if the application is started successfully, as shown by block 452, then the VSP service 424 will activate a second APN interface, as shown by message 460. From Figure 4, the virtual lines and bill split are now set up and ready to use.
[0065] The second data APN that is added to the enterprise_unsecure FIB may be represented as a logical interface in the system. The new work cellular interface is not secure since it is not pushed from an enterprise server and is over an unsecured carrier network.

[0066] The new interface may be assigned a type or label such as "cellular_work". This type allows the system services that deal directly with interfaces to be able to differentiate personal cellular and work cellular interfaces. In order to support such new interface, a new routing domain or FIB may be added in a multi-FIB device. For example, such new FIB may be considered a "enterprise_unsecure" FIB since it is was pushed by a carrier and is therefore considered by the enterprise to be an unsecure connection.

[0067] In this case, secure data may be sent over a separate interface, labelled as "enterprise_secure". Previously all unsecured communication would go over a personal connection. However, for billing purposes, now an enterprise_unsecure routing domain is provided to allow for certain data communications to be processed over such unsecured communication. The work cellular interface is then added to this FIB and other interfaces such as Wi-Fi or VPN interfaces from the Personal FIB may also be added to the new FIB.

[0068] Applications may then be assigned to the new FIB based on a group identifier associated with the application. Specifically, applications are assigned a group ID associated with a FIB. In many cases, an application will have a single group ID associated with a single FIB. However, in some cases hybrid applications or services may access multiple FIBs by having multiple group IDs associated with such application. Further, applications may be hybrid in which case they would permit communications over the enterprise_unsecure FIB or personal FIB.

[0069] In some situations, preference may be given to a particular FIB for hybrid applications. Such preference may be utilized, for example, to select a Enterprise FIB first. However, if the Enterprise FIB is overly busy or causes significant delay then a personal FIB may be utilized instead.

[0070] After such enterprise_unsecured FIB has been put on to the device, all data traffic that is routed over this FIB may then be accurately captured by the carrier and billed to the enterprise rather than to the personal account of the mobile device holder.

[0071] By using multiple routing domains or forward information bases, each perimeter or personality on the device may have its own routing table or domain, its own interface and its own interface priorities. In this case, traffic that proceeds over a personal FIB has different routing in place than traffic over other FIBs. Separate interface priorities allow a default route interface to be different for each FIB. This architecture also adds an extra level of security by not exposing interfaces to other FIBs.

[0072] Reference is now made to Figure 5, which is a data flow diagram showing the enablement of voice on the VSP service. In particular, as seen in Figure 5, a carrier includes a VSP server 330 which may communicate with UE 512.

[0073] UE 512 includes a VSP service 520 and a VSP application 522. A user 524 may in some cases be required to approve the services or activation of the services on the UE 512.

[0074] In particular, as seen in Figure 5, a VSP service 520, when starting, may provide a notification to the user 524 as shown by message 530. Such message may be provided to the user to indicate whether or not it is acceptable to start the service. If the user approves, as shown by message 532, then the VSP application 522 may provide a notification 540 to the VSP server 330.

[0075] Once notification 540 is received, VSP server 330 may then, optionally, provide verification messages to user 524. These are shown by message 542 providing a text message to user 524 to confirm a PIN. A user confirmation is shown by message 544.

[0076] Messages 542 and 544 are optional. In other embodiments, when notification 540 is received by VSP server 330, VSP server 330 may automatically indicate to the VSP application 522 to continue.

[0077] In the embodiment of Figure 5, if the PIN is okay then a message to continue is sent, as shown by message 550. VSP application 522 receives message 550 and requests a VSP profile for the UE 512, as shown by message 552.

[0078] VSP profile may include the secondary (or virtual) phone number and other information for the device and may be pushed to the device in message 554.

[0079] VSP application 522 receives message 554 and stores the VSP profile in a VSP profile database 560. Such storing is shown by message 562.

[0080] The VSP application 522 may then provide the VSP profile to the VSP service 520, as shown by message 564. The VSP service 520 may then store the VSP profile as a persistent object in the operating system of the UE 512, shown by message 570. The persistent object store is shown by block 572 in the embodiment of Figure 5.

[0081] At this point, the line provider is up, as shown by block 580 and the secondary phone number may be utilized.

[0082] In some cases, the VSP profile of message 554 may be enabled by the enterprise server. In particular, the enterprise server may request certain phone numbers or reserve certain phone numbers and other information from the VSP server 330 to be pushed to UE 512.

[0083] The persistent objects within the operating system at block 572 may control the profile for certain uses. For example, the user interface may be changed on the device to allow for the calling from different numbers. Thus, an option may be given to user to phone from a first number from a second number. Further, text messaging or SMS applications may also be provided with two different numbers, and in some cases two different inboxes or application spaces may be provided for such
separate SMS numbers. In some cases the first number may be used for a first bill and the second number may be used for a second bill.

[0084] Reference is now made to Figure 6 which shows data enablement for the second APN. In particular, work data may flow over the second APN, as described above.

[0085] As seen in Figure 6, a UE 610 includes the VSP service 612 that was installed, for example, as described in regards to Figure 4. The device further includes a cellular services module 614, as well as a network stack 616.

[0086] In the embodiment of Figure 6, once the second phone line is activated, the VSP service 612 may request the activation of the second APN interface from the cellular services module 614, as shown by message 620.

[0087] Cellular services module 614 receives message 620 and initiates the creation of the interface for the FIB as described above with the network stack 616, as shown by message 622. Message 622 may include information such as the interface, the FIB, and the type label, for example.

[0088] Once the persistent object has been stored, an acknowledgement 626 may be provided. The interface is then provided from the cellular service 614 to the VSP service 612, as shown by message 630.

[0089] The creation of the interface and the FIB may result in several factors. For data, once the data is enabled over the second APN, certain applications may select connections with the cellular work FIB as needed. For example, a VPN manager may be set to prefer the cellular work interface.

[0090] Further, certain device specific connections may also be set to select work cell connections as needed.

[0091] Further, enterprise_unsecured FIBs may have the personal cellular interface removed and the work cellular interface added, thereby ensuring that enterprise_unsecured messages are billed to the cellular work bill. Until the service is activated, exiting applications that normally would send enterprise_unsecure traffic would use a personal cellular interface in the enterprise_unsecure FIB to ensure they still have connectivity. In this way, when the VSP service is enabled, the application does not need to change.

[0092] While the above describes the creation and setting up of the second phone line and data APN, the device also may have procedures for power up and deletion of the services.

[0093] In particular, reference is now made to Figure 7, which shows a process on a device for power up. As seen in Figure 7, UE 710 includes VSP service 712. On power up, the device first checks and listens to the enterprise management agent, for example enterprise management agent 412 from Figure 4 above, to determine whether or not the VSP information is okay, as shown by block 720.

[0094] If yes, the process of Figure 7 proceeds to block 722 in which a check is made to determine whether the VSP information and the VSP profile are okay against the particular SIM that is inserted in the device. If yes, the process proceeds to block 724 in which the persistent objects are added and the line provider is brought up.

[0095] Once the line is active, the APN information is then checked as shown by block 626 in Figure 6. If the second APN is okay then VSP status is set to enabled.

[0096] The process then proceeds to block 730 in which and the second APN interface is activated.

[0097] If any of the steps fail, then the VSP service is disabled and the device may consider that it is waiting for new VSP information from the enterprise server.

[0098] If, for example, a new SIM is inserted into the device, the new SIM may also be enabled for VSP. In this case, the enterprise server may also provide any new identifier such as the IMSI and the process as outlined in Figure 4 may proceed to initialize the VSP service.

[0099] In a further embodiment, a VSP service may need to be deleted from a device. Reference is now made to Figure 8. In particular, UE 810 may no longer be needed to use an enterprise. For example, the employee may leave the workplace and the employer may wish to remove the VSP service from the device.

[0100] In this regard, UE 810 communicates with enterprise server 814 using EMA 816 on the UE.

[0101] UE 810 further includes VSP service 812.

[0102] Enterprise server 814 may send a delete VSP command with information regarding the VSP service to the enterprise management agent 816, as shown by message 820. Enterprise management agent 816 may acknowledge message 820, as shown by message 822.

[0103] Enterprise management agent 816 then triggers the VSP service 812 to perform the deletion of the VSP application and settings. In particular, as shown by Figure 8, the VSP service 812 listens to the enterprise management agent for VSP information and sees a deletion request, as shown by block 830. The VSP service 812 then sets the enablement of the VSP service to false as shown by block 832.

[0104] The VSP service 812 may then de-activate the second APN interface as shown by arrow 840 and may then delete the VSP profiles, take down line providers, remove the persistent objects in the operating system (including received SMS texts), among other tasks, as shown by block 842.

[0105] In one embodiment, the app may not be deleted. In other embodiments, the app may be deleted and may need to be retrieved again upon the device being connected to an enterprise server requiring the VSP services.

[0106] From Figure 8 above, the deactivating of the second APN may be accomplished in accordance with Figure 9. As seen in Figure 9, UE 910 includes VSP service 912, cellular services modules 914 and the network stack 916.

[0107] In disabling the dual APN data, the VSP service 912 sends a message 920 to the cellular services module
In which the device starts the VSP process. Such starting can include the configuration of the VSP process as described in Figure 4 above.

From block 1014 the process proceeds to block 1016 in which the VSP service is verified. Such verification may include verifying the IMSI of the device and the PIN as described above.

From block 1016, the process proceeds to block 1020 in which the VSP daemon starts the data networking APN based on the configuration information for the carrier. The process then proceeds to block 1022 in which a system indicator is set indicating that the VSP is configured.

From a carrier perspective, the carrier does not enable or configure the APN until after the data networking APN is started on the UE. In this way, resources at the carrier are not wasted by having preconfigured APNs for devices that may not use them.

The process then proceeds to block 1030 in which a check is made to see whether or not the service has been disabled. If no, the process continues to loop to block 1030.

Conversely, once the service is shut down, the process proceeds to block 1032 in which the system indicator is set to disable the second APN and the process then proceeds to block 1034 in which the data networking APN is stopped. From block 1034 the process proceeds to block 1040 and ends.

The above therefore provides for split billing between a personal and work space by first starting the VSP service for voice, and once the VSP service for Voice is started, configuring the second data APN between the UE and the carrier.

While the above is described with regards to a work and personal space, the split billing could equally be used for a device having two or more users, where each user has application associated with them. In this way, each user could obtain a bill for the voice and data each uses on the device.

Further, while the above is described with regards to two spaces, in some embodiments more than two APNs and phone numbers could be associated with a device, and more than two bills generated. The startup and shut down procedures for a many identities is similar to that described above with regards to Figure 4 to 10.

The above may be implemented on any computing device. If the above is implemented on a user equipment, one example is provided with regard to Figure 11.

UE 1100 may be a two-way wireless communication device having voice and data communication capabilities. Depending on the exact functionality provided, the UE may be referred to as a data messaging device, a two-way pager, a wireless e-mail device, a cellular telephone with data messaging capabilities, a wireless Internet appliance, a wireless device, a mobile device, or a data communication device, as examples.

Where UE 1100 is enabled for two-way communication, it may incorporate a communication subsys-
tem 1111, including both a receiver 1112 and a transmitter 1114, as well as associated components such as one or more antenna elements 1116 and 1118, local oscillators (LOs) 1113, and a processing module such as a digital signal processor (DSP) 1120. Although not shown, communication subsystem 1111 may include additional components. For example, UE 1100 may comprise multiple receivers 1112 and/or transmitters 1114 to allow for simultaneous radio activity. In addition, as will be apparent to those skilled in the field of communications, the particular design of the communication subsystem 1111 will be dependent upon the communication network in which the device is intended to operate.

[0130] Network access requirements will also vary depending upon the type of network 1119. In some networks network access is associated with a subscriber or user of UE 1100. A UE may require one or more smart cards which can contain different applications such as a USIM, RUIM or a SIM application in order to operate on a network. The smart card interface 1122 both communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 1132 and display 1122, for example, may be used for both communication-related functions, such as entering a text message for transmission over a communication network, and device-resident functions such as a calculator or task list.

[0135] Operating system software used by the processor 1138 may be stored in a persistent store such as flash memory 1124, which may instead be a read-only memory (ROM) or similar storage element (not shown). Those skilled in the art will appreciate that the operating system, specific device applications, or parts thereof, may be temporarily loaded into a volatile memory such as RAM 1126.

[0136] As shown, flash memory 1124 can be segregated into different areas for both computer programs 1158 and program data storage 1150, 1152, 1154 and 1156. These different storage types indicate that each program can allocate a portion of flash memory 1124 for their own data storage requirements. Processor 1138, in addition to its operating system functions, may enable execution of software applications on the mobile device. A predetermined set of applications that control basic operations, including at least data and voice communication applications for example, will normally be installed on UE 1100 during manufacturing. Other applications could be installed subsequently or dynamically.

[0137] Applications and software may be stored on any computer readable storage medium. The computer readable storage medium may be a tangible or in transitory/non-transitory medium such as optical (e.g., CD, DVD, etc.), magnetic (e.g., tape) or other memory known in the art.

[0138] One software application may be a personal information manager (PIM) application having the ability to organize and manage data items relating to the user of the UE such as, but not limited to, e-mail, calendar events, voice mails, appointments, and task items. Naturally, one or more memory stores would be available on the UE to facilitate storage of PIM data items. Such PIM application may have the ability to send and receive data items, via the wireless network 1119. Further applications may also be loaded onto the UE 1100 through the network 1119, an auxiliary I/O subsystem 1128, serial port 1130, short-range communications subsystem 1140 or any other suitable subsystem 1142, and installed by a user in the RAM 1126 or a non-volatile store (not shown) for execution by the processor 1138. Such flexibility in application installation increases the functionality of the
device and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the UE 1100.

[0139] In a data communication mode, a received signal such as a text message or web page download will be processed by the communication subsystem 1111 and input to the processor 1138, which may further process the received signal for output to the display 1122, or alternatively to an auxiliary I/O device 1128.

[0140] A user of UE 1100 may also compose data items such as email messages for example, using the keyboard 1132, which may be a complete alphanumeric keyboard or telephone-type keypad, whether virtual or real, among others, in conjunction with the display 1122 and possibly an auxiliary I/O device 1128. Such composed items may then be transmitted over a communication network through the communication subsystem 1111.

[0141] For voice communications, overall operation of UE 1100 is similar, except that received signals would typically be output to a speaker 1134 and signals for transmission would be generated by a microphone 1136. Alternative voice or audio I/O subsystems, such as a voice message recording subsystem, may also be implemented on UE 1100. Although voice or audio signal output is generally accomplished primarily through the speaker 1134, display 1122 may also be used to provide an indication of the identity of a calling party, the duration of a voice call, or other voice call related information for example.

[0142] Serial port 1130 in Figure 11 would normally be implemented in a personal digital assistant (PDA)-type UE for which synchronization with a user’s desktop computer (not shown) may be desirable, but is an optional device component. Such a port 1130 would enable a user to set preferences through an external device or software application and would extend the capabilities of UE 1100 by providing for information or software downloads to UE 1100 other than through a wireless communication network. The alternate download path may for example be used to load an encryption key onto the device through a direct and thus reliable and trusted connection to thereby enable secure device communication. As will be appreciated by those skilled in the art, serial port 1130 can further be used to connect the UE to a computer to act as a modem. Other communications subsystems 1140, such as a short-range communications subsystem, is a further optional component which may provide for communication between UE 1100 and different systems or devices, which need not necessarily be similar devices. For example, the subsystem 1140 may include an infrared device and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices. Subsystem 1140 may further include non-cellular communications such as Wi-Fi or WiMAX.

Claims

1. A method at a user equipment (302; 410) to facilitate activation and splitting of data billing between at least two parties, the method comprising:

starting (442; 1014), at the user equipment, a virtual subscriber identity module platform, VSP, service (424) on the user equipment, the user equipment being configured with a first data networking Access Point Name, APN, for a carrier network;

verifying (444; 1016) VSP configuration information with a network server;

upon verification, starting (460; 1020) a second data networking APN for the same carrier network based on the configuration information on the user equipment; and

setting (1022) a status indicator on the user equipment to indicate the VSP service is enabled.

2. The method of claim 1, wherein VSP configuration information includes an international mobile subscriber identity from a physical universal integrated circuit card, UICC, subscriber identity module, SIM, application.

3. The method of claim 1 or 2, wherein the network server (313; 412) is an enterprise management agent, EMA, server.

4. The method of any preceding claim, wherein the starting of the VSP service is based on a policy received from an enterprise server (313; 412).

5. The method of claim 4, wherein the at least two parties include a user of the user equipment and an enterprise.

6. The method of any preceding claim, wherein the starting includes associating a forwarding information base, FIB, for the data networking APN with applications on the user equipment.

7. The method of any preceding claim, further comprising, when one of the at least two parties leaves the splitting of data billing, deactivating the APN.

8. The method of claim 7, wherein the deactivating includes setting the status indicator on the user equipment to indicate the VSP service is disabled.

9. A user equipment (302; 410) configured to facilitate activation and splitting of data billing between at least two parties, the user equipment comprising

a processor; and
a communications subsystem,

wherein the user equipment is configured to carry out the method of any one of claims 1 to 8.

10. A computer program comprising instructions that, when executed by a processor of a user equipment, are configured to facilitate activation and splitting of data billing between at least two parties by carrying out the method of any one of claims 1 to 8.

Patentansprüche

1. Verfahren an einem Endgerät (302; 410), um die Aktivierung und Aufteilung einer Datenabrechnung zwischen mindestens zwei Parteien, wobei das Verfahren folgende Schritte umfasst:

   Starten (442; 1014), an dem Endgerät, eines Dienstes (424) einer Plattform eines virtuellen Teilnehmeridentitätsmoduls, VSP, auf dem Endgerät, wobei das Endgerät mit einem ersten Zugangspunktnamen, APN, zur Datenvernetzung für ein Trägernetzwerk konfiguriert ist;
   Überprüfen (444; 1016) von VSP-Konfigurationen bei einem Netzwerkservice;
   nach der Überprüfung, Starten (460; 1020) eines zweiten Datenvernetzungs-APN für das gleiche Trägernetzwerk basierend auf den Konfigurationen auf dem Endgerät; und
   Einstellen (1022) eines Statusindikators auf dem Endgerät, um anzugeben, dass der VSP-Dienst aktiviert ist.

2. Verfahren nach Anspruch 1, wobei die VSP-Konfigurationen eine internationale Mobilteilnehmeridentität von einer Anwendung eines Teilnehmeridentitätsmoduls, SIM, einer physischen universellen IC-Karte, UICC, umfassen.

3. Verfahren nach Anspruch 1 oder 2, wobei der Netzwerkservice (313; 412) ein Unternehmensmanagementagenten-, EMA, Server ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei das Starten des VSP-Dienstes auf einer Politik basiert, die von einem Unternehmensserver (313; 412) empfangen wird.

5. Verfahren nach Anspruch 4, wobei die mindestens zwei Parteien einen Benutzer des Endgeräts und ein Unternehmen umfassen.


7. Verfahren nach einem der vorhergehenden Ansprüche, ferner umfassend, wenn eine der mindestens zwei Parteien das Aufteilen der Datenabrechnung verlässt, das Deaktivieren des APN.

8. Verfahren nach Anspruch 7, wobei das Deaktivieren das Einstellen des Statusindikators auf dem Endgerät, um anzugeben, dass der VSP-Dienst deaktiviert ist, umfasst.

9. Endgerät (302; 410), konfiguriert, um die Aktivierung und Aufteilung einer Datenabrechnung zwischen mindestens zwei Parteien zu ermöglichen, wobei das Endgerät umfasst

   einen Prozessor; und
   ein Kommunikationsteilsystem,
   wobei das Endgerät konfiguriert ist, um das Verfahren nach einem der Ansprüche 1 bis 8 durchzuführen.

10. Computerprogramm, das Anweisungen umfasst, die, wenn sie durch einen Prozessor eines Endgeräts ausgeführt werden, konfiguriert sind, um die Aktivierung und Aufteilung der Datenabrechnung zwischen mindestens zwei Parteien zu ermöglichen, indem das Verfahren nach einem der Ansprüche 1 bis 8 durchgeführt wird.

Revendications

1. Procédé au niveau d’un équipement utilisateur (302 ; 410) pour faciliter une activation et une division de facturation de données entre au moins deux parties, le procédé comprenant :

   démarrer (442 ; 1014), au niveau de l’équipement utilisateur, un service de plateforme de module d’identité d’abonné virtuel, VSP, (424) sur l’équipement utilisateur, l’équipement utilisateur étant configuré avec un premier nom de point d’accès, APN, de réseautage de données pour un réseau porteur ;
   vérifier (444 ; 1016) des informations de configuration de VSP avec un serveur de réseau ;
   après la vérification, démarrer (460 ; 1020) un second APN de réseautage de données pour le même réseau porteur sur la base des informations de configuration sur l’équipement utilisateur ; et
   régler (1022) un indicateur d’état sur l’équipement utilisateur pour indiquer que le service de VSP est activé.

2. Procédé selon la revendication 1, dans lequel des
informations de configuration de VSP comprennent une identité internationale d'abonné mobile provenant d’une application de module d'identité d'abonné, SIM, de carte de circuits intégrés universelle physique, UICC.

3. Procédé selon la revendication 1 ou 2, dans lequel le serveur de réseau (313 ; 412) est un serveur d’agent de gestion d’entreprise, EMA.

4. Procédé selon une quelconque revendication précédente, dans lequel le démarrage du service de VSP est basé sur une politique reçue en provenance d’un serveur d’entreprise (313 ; 412).

5. Procédé selon la revendication 4, dans lequel les au moins deux parties comprennent un utilisateur de l’équipement utilisateur et une entreprise.

6. Procédé selon une quelconque revendication précédente, dans lequel le démarrage comprend l’association d’une base d’informations de transfert, FIB, pour l’APN de réseautage de données avec des applications sur l’équipement utilisateur.

7. Procédé selon une quelconque revendication précédente, comprenant en outre, lorsque l’une des au moins deux parties quitte la division de facturation de données, la désactivation de l’APN.

8. Procédé selon la revendication 7, dans lequel la désactivation comprend le réglage de l’indicateur d’état sur l’équipement utilisateur pour indiquer que le service de VSP est désactivé.

9. Equipement utilisateur (302 ; 410) configuré pour faciliter une activation et une division de facturation de données entre au moins deux parties, l’équipement utilisateur comprenant
   un processeur ; et
   un sous-système de communication,
   l’équipement utilisateur étant configuré pour mettre en oeuvre le procédé selon l’une quelconque des revendications 1 à 8.

10. Programme d’ordinateur comprenant des instructions qui, lorsqu’elles sont exécutées par un processeur d’un équipement utilisateur, sont configurées pour faciliter une activation et une division de facturation de données entre au moins deux parties par mise en oeuvre du procédé selon l’une quelconque des revendications 1 à 8.
FIG. 1
<table>
<thead>
<tr>
<th>Flags</th>
<th>UG</th>
<th>UC</th>
<th>UHL</th>
<th>UH</th>
<th>lo0</th>
<th>lo1</th>
<th>link#6</th>
<th>link#7</th>
<th>link#8</th>
<th>link#9</th>
<th>link#10</th>
<th>link#11</th>
<th>link#12</th>
<th>link#13</th>
<th>link#14</th>
<th>link#15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>254.890.206</td>
<td>254.90.207</td>
<td>127.0.0.1</td>
<td>127.0.0.2</td>
<td>127.0.0.3</td>
<td>169.254.208.100/30</td>
<td>169.254.208.102</td>
<td>169.254.208.103</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet:</td>
<td>254.890.204/30</td>
<td>254.90.206</td>
<td>127.0.0.1</td>
<td>127.0.0.2</td>
<td>127.0.0.3</td>
<td>169.254.208.100/30</td>
<td>169.254.208.102</td>
<td>169.254.208.103</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>254.890.206</td>
<td>254.90.206</td>
<td>127.0.0.1</td>
<td>127.0.0.2</td>
<td>127.0.0.3</td>
<td>169.254.208.100/30</td>
<td>169.254.208.102</td>
<td>169.254.208.103</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FIG. 2
FIG. 3

UEs 302

Carrier Network 303

Firewall 305

Relay 307

VSP 330

Enterprise Server 313

Secure Channel 309

Firewall 311

Network Operation Center 308

Internet 320

MDS Server 315
FIG. 6

Network Stack 616

Cellular Services 614

VSP Service 612

Activate 2nd APN I/F 620

Net connect

ACK

IF identity for VSP 630

UE 610
FIG. 7

- VSP Service 712
  - Check for or listen to EMA VSP Info 720
  - Check if VSP info and profile are ok 722
  - Add persistent objects and line provider 724
  - Check APN info and if ok set VSP status to enable 726
  - Activate 2nd APN interface 730

UE 710
FIG. 8

Enterprise Server 814

Delete VSP Info 820

ACK 822

EMA 816

VSP Service 812

Listen to EMA VSP Info, see delete 830
Set VSP status to disable 832
Deactivate 2nd APN V/F 840
Delete VSP profiles, take down line providers, remove persistent objects 842
FIG. 9

VSP Service 912

Deactivate 2nd APN I/F 920

Cellular Services 914

Net disconnect 922

ACK 926

Network Stack 916

UE 910
FIG. 10

Flowchart:

1. Start
2. Start VSP
3. Verify VSP Service
4. Start Data Networking APN
5. Set VSP Status indicator to enabled
6. VSP Disabled?
7. N
8. Y
9. Set VSP Status indicator to disabled
10. Stop Data Networking APN
11. End
REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- US 8996002 B2 [0005]
- JP 2011192129 A [0006]
- US 20120108204 A [0008]