

MANAGING MOBILE DEVICE IDENTITIES

Field of the Invention

The invention relates to telecommunications, and specifically to the management of identity
5 in mobile devices attaching to telecommunications networks.

Background to the Invention

A primary customer identity is usually a unique human being but can be a machine, or
sometimes a company entity such as a department. On a telecommunications network itself,
10 identity is represented by one or more identifiers recognised by elements of, or attached to,
the network. In the context of mobile telecommunications, such identifiers are commonly the
customers IMSI (International Mobile Subscriber Identity) that resides on a
SIM (Subscriber Identity Module), a telephone number MSISDN (Mobile Subscriber
Integrated Services Digital Network Number), or other important identities such as MAC
15 (Media Access Control) address, IP address, email address and IMEI (International Mobile
Equipment Identity).

In the GSM (Global System for Mobile communication) authentication is performed using a
SIM inserted into the mobile communications device. This manages the connection to the
20 network as well as the user identity and the network subscriber keys. There are two types of
network service – home service and roaming service.

‘Roaming’ refers to extending the connectivity of a service to a location that is different from
a home location. When a mobile communications device, such as a mobile telephone,
25 travels with a user outside of their home operator coverage area – ‘territory’ - the device can
still access services using roaming mechanisms/services. However, there are a growing
number of people who live in more than one home and, of course, machines such as
airplanes and cars don’t have a ‘home’ in the human sense of the word. Such users are
poorly served by current systems.

Another problem travellers experience as they travel near country or region borders is that
mobile phones may inadvertently attach to a foreign network, even though they may be
physically in a home territory. Under normal operation, once a handset (i.e. a mobile phone)
is attached to a network, it remains attached to it until signal is lost or if the subscriber
35 manually disconnects. As a result, the user is charged high roaming charges for an extended
period even if though they were physically in their home territory. In some regions such as

Canada, USA and India where there is national roaming this effect can lead to accidentally high bills even when the customer is not travelling at all.

There are few options available to users when travelling which help reduce these
5 surcharges:-

One option for a user is to purchase a plurality of additional pre-pay subscriber identification modules (SIMs), one for each territory which the user visits. A SIM is a plastic card with embedded electronic circuitry, which has a unique serial number and an international
10 number for the mobile user (IMSI). The SIM enables communication between the mobile device and available cellular networks. Therefore, by purchasing a plurality of different SIMs, - one for each territory - the user is able to replace the original SIM with an appropriate SIM for the territory being visited. In this way, the mobile device appears to be a subscriber of the foreign network, which means the user can make and receive calls or use data services
15 without incurring roaming surcharges.

This option has many disadvantages:

- The user must purchase and carry around a plurality of different SIM cards;
- The user must ensure that there is sufficient credit in the accounts linked with each
20 SIM card. Furthermore, it is not desirable to have unused credit on a number of different networks, as this credit may be wasted without being redeemed;
- The act of maintaining a plurality of different SIM accounts is cumbersome and time consuming, involving considerable user interaction;
- When the Subscriber swaps SIM their mobile number changes this means they are
25 no longer reachable on their normally used number. Further if they make an outbound call their Caller Line Identifier (CLI) will be a new one and therefore unknown to the receiver. This may result in the called party refusing to answer that call as they do not recognise the caller.
- Law enforcement agencies are frustrated in their endeavours to keep track of
30 undesirable people as they effectively have to keep track of multiple copies of the same person.

There are attempts in the prior art to address at least some of these problems.

35 WO2006/002951 (Brunnekreef) relates to an approach in which the user (or an application) on the mobile phone can pre-pend a (sometimes hidden) telephone number of an

intermediate service that will accept the user's call, remove the pre-pended information and call the desired destination number. The caller then drops the call automatically and awaits a call-back. The intermediate service calls the user back to complete the connection, and this may give the user better calling rates than normal roaming surcharges. This has the disadvantage of introducing a delay in the communication channel while the user is trying to contact another party. Furthermore, the user gets a very poor user experience due to handset software compatibility issues: depending on the model of the mobile phone, the phone may appear to 'do nothing' until it gets the call back, strange messages such as 'call failed' or 'call blocked' may appear or the service may not work at all.

Another prior art approach is to have a mechanical device that includes a flexible strip (often called a slim SIM). This device physically connects multiple SIMs to a handset, and can be used with a means of switching between the SIMs. This device requires there to be some spare space within the handset to store the additional SIMs, and this solution is problematic to implement if the SIMs are not compatible with each other (e.g. use different data speeds or voltages). Alternately the Images of all but one SIM can be cloned onto the SlimSIM chip and a remaining SIM used – a one plus many clones solution. Again the physical form factor is incompatible with many handsets and the cloning of SIMs is unlawful in many countries and breaks contracts in almost all cases.

Multi-IMSI SIMs are available that offer the capability of being pre-programmed with a plurality of mobile subscriber data sets. The data sets are sometimes incorrectly referred to as IMSIs, hence the name 'multi-IMSI SIM', but are actually data sets which each comprise an international mobile subscriber identity (IMSI) and other network-related data. These SIMs have processing capability and an algorithm to present the correct set of data to the phone based on the location of that phone. This allows the phone to present as a 'local' subscriber to the network in question.

Many fixed format Dual and Multiple IMSI SIM systems have been sold by companies such as VeriSign and Gemalto and these are described in various patent applications such as Cammilleri (WO2007102003), Stadelmann (WO9955107), Salomon (WO0221872), Bongers (WO0049820). In such systems, a piece of software runs in the SIM or on the handset or a separate electronic module and makes decisions as to which IMSI to use given the location and available networks. Such systems are sometimes called SmartSIMs, but in fact this is a misnomer as all SIMs are smart and contain a microprocessor and memory to run network selection and authentication programs.

Such systems are however typically relatively inflexible to changes in network availability over time and require informed decision making from users. This can result in failures of operation and poor network choices.

- 5 An improved system is disclosed in the applicant's earlier WO 2011/036484. This discloses a system in which a central service – an “IMSI Broker” – is adapted to provision the SIM of a mobile handset with new identities as required. While this approach addresses certain problems of the prior art, it does not in itself solve the problem of making reliable and effective choices of identity at the mobile handset.

10

Summary of Invention

- In a first aspect, the invention provides a method of managing identities for use in a mobile telecommunications device in a telecommunications network, the method comprising:
- 15 triggering an identity management process; detecting one or more parameters associated with the mobile telecommunications device; in the identity management process, selecting an identity management rule determined by the one or more parameters detected; in the identity management process, searching an identity database wherein each record comprises an identity and additional identity information for each identity, wherein the searching prioritises records according to the identity management rule; in the identity
- 20 management process, selecting an identity when a record conforming to the identity management rule is found in said searching; and in the identity management process, modifying an active identity of the mobile telecommunications device to be the selected identity when the active identity is not already the selected identity.

- 25 This method is particularly effective as the present inventors have determined that parameters associated with the mobile telecommunications device itself, rather than just those relating to location, may be particularly important to identity choice. This is because it is found that some identities (because, for example, of the properties or method of operation of associated telecommunications networks) are particularly effective or less prone to
- 30 problems than others for particular mobile telecommunications devices.

Preferably each said identity comprises an IMSI.

- The one or more parameters comprise a handset type. This may be as determined from the
- 35 TAC code in the IMEI of the handset. The one or more parameters may also comprise a subscription type associated with the device, wherein the subscription type relates to one or more of a device operating system and a communication type. These parameters allow for

an effective choice of identity to avoid difficulties which may occur with particular combinations of mobile communications device and network.

The additional information may comprise an MCC and an MNC for each identity. If so, it is advantageous for the identity management rule to allow for selection of an identity based on matching of some or all of an MCC or an MNC value. If there is no match established by the identity management rule to a specific identity, a new identity may be selected from a pool of matching identities.

Advantageously, a process of modifying the active identity is determined according to the one or more parameters of the device. This allows modification of the active identity to be carried out effectively in accordance with the capabilities of the device itself.

Advantageously, if on modifying the active identity no service is provided to the new active identity, the active identity is modified to a backup identity different from the identity for which no service was provided. This ensures that the device is not fixed with an identity which is theoretically the best, but which has in practice a service problem – with this approach, service will still result even if the initial identity choice is ineffective.

In a further aspect, the invention provides a subscriber identity module for use in a mobile telecommunications device and having a plurality of identities for use in a mobile telecommunications network, the subscriber identity module comprising a memory and a processor, wherein the memory comprises an identity management process for execution by the processor and an identity database, wherein the processor is adapted to: on triggering, initiate the identity management process; detect one or more parameters associated with the mobile telecommunications device; in the identity management process, selecting an identity management rule determined by the one or more parameters detected; in the identity management process, search an identity database wherein each record comprises an identity and additional identity information for each identity, wherein the searching prioritises records according to the identity management rule; in the identity management process, select an identity when a record conforming to the identity management rule is found in said searching; and in the identity management process, modify an active identity of the mobile telecommunications device to be the selected identity when the active identity is not already the selected identity.

Brief Description of Drawings

Specific embodiments of the invention will be described below, by way of example, with reference to the accompanying drawings, of which:

Figure 1 is an overview of a conventional communications system in which aspects of the present invention can operate;

Figure 2 is a functional block diagram of a system in which identities may be provided by a central service, and also show the elements of a SIM in accordance with embodiments of the invention;

Figure 3 shows elements of an identity management process in accordance with one aspect of the invention;

Figure 4 illustrates different possible trigger steps in the process of Figure 3, and their consequences;

Figure 5 illustrates an IMSI selection procedure for use in the process of Figure 3;

Figure 6 illustrates a process for managing an IMSI pool for use in the IMSI selection procedure of Figure 5; and

Figure 7 illustrates a data record structure for use in the process of Figure 3.

Detailed Description of Preferred Embodiments

Figure 1 provides a schematic representation of two cellular telecommunications networks, one in the UK and one in Italy, to indicate the general roaming problem addressed by embodiments of the invention. In reality there are many more Mobile Network Operators (MNO), Mobile Virtual Network Operators (MVNO) or Mobile Virtual Network Enablers (MVNE), and as such many more cellular telecommunications networks. However, Figure 1 represents only two networks for simplicity.

When a first user makes a call from a first mobile phone 10 in the first user's local network, for example, in the UK, to a second user 20 in a foreign network (i.e. Italy), the call is routed through the local network's base station subsystem (BSS) 30 to a local network switching subsystem (local-NSS) 32, the call is then routed through the Signaling System Number 7 (SS7) 34 network to the foreign network, and through a foreign network switching subsystem (foreign-NSS) 36 to the foreign network's base station subsystem 38. The call is finally routed to the second user's mobile phone 20. Calls in the opposite direction are routed in the same way, through the foreign network's base station subsystem, to the foreign network switching subsystem 36, through SS7 34 to the local network switching subsystem (local-NSS) 32, on to the local network's base station subsystem (BSS) 30, and finally to the first mobile phone 10.

The way that the call is routed to the correct recipient is through a plurality of location registers which form part of the network subsystems. For every user registered in a particular cellular telecommunications network, there is a record held in that network's Home Location Register (HLR) 40, 42. The HLR 40,42 is a central database that contains details of each mobile phone subscriber that is authorized to use that particular network.

The HLR stores details of every Subscriber Identity Module (SIM) card issued by the mobile phone operator (i.e. MNO, MVNO or MVNE). A SIM is a plastic card with embedded electronic circuitry, which is inserted into the mobile phone. Each SIM has a unique identifier called an International Mobile Subscriber Identity (IMSI) which is a primary key to each HLR record. IMSIs are used in *any* mobile network that interconnects with other networks, including CDMA and EVDO networks as well as GSM networks.

An IMSI is usually 15 digits long, but there are some exceptions. Typically the first 3 digits are the Mobile Country Code (MCC), followed by the Mobile Network Code (MNC), (either 2 digits (European standard) or 3 digits (North American standard)). The remaining digits contain a mobile station identification number (MSIN) within the network's customer base.

SIMs also comprise one or more MSISDNs, which are the telephone numbers used by mobile phones to make and receive calls. Each MSISDN is also a primary key to the HLR record.

In summary, there is a relationship between the HLR, MSISDN, IMSI, and the SIM. The SIM is the physical device which contains a record of the IMSI. The MSISDN is the unique number identifying the mobile phone. The IMSI is the unique identifier of the user subscribing to the network, and the HLR is the system that maps MSISDNs to IMSIs and vice versa.

The above holds true when a user 'roams' away from their home/local network to a foreign network also called a roamed-to network. However, when a mobile phone attempts to connect to a network which is not the home/local network, the roamed-to network communicates with the home network in order to verify whether the mobile phone is authorised to use the roamed-to network. This communication is possible because there are reciprocal agreements between many of the available network operators.

When a user roams away from their home service and into an area served by another operator, messages are exchanged over the SS7 network and the roamed-to network operator obtains information from the home network's HLR and creates a temporary record for the subscriber in its Visitor Location Register (VLR) 44, 46. The VLR is a database which is maintained by a network operator (in the same way as the HLR is maintained). However, the VLR of the Mobile Switching Center (MSC) contains temporary information about mobile users that are currently located within the service area of that MSC.. When calls are made from the mobile phone, the VLR is checked for authorisation, and assuming authorisation is permitted, the Mobile Switching Center (MSC) permits tracking of the use of the mobile phone for billing purposes. The HLR subscriber profile (i.e. which services are allowed) is downloaded to the VLR when subscribed user registers on (connects to) the network (same for roaming and home network). All call handling and billing related call data record (CDR) generation is done by the MSC - the HLR is not involved.

So using the example in Figure 1, a user subscribed to a mobile network operator in the UK visits Italy. When the user arrives in Italy and turns on the mobile phone, the mobile phone will try to connect to an available Italian network operator 36. The Italian network operator can identify from the IMSI number stored in the SIM card that the user is not subscribed to the Italian network, and as such, will contact the user's home network 32 in the UK to verify whether the user is authorised to use the Italian network.

The VLR 46 updates the HLR 40 in the UK, with location information over SS7 with a Location Update message (LU). The LU message is routed to the HLR(UK) based on the global title translation of the IMSI that is contained in a Signalling Connection Control Part (SCCP) field of the LU. The HLR(UK) informs the VLR(IT) as to the status of the subscriber and whether service is to be provided in the roamed-to network, i.e. the Italian network. If the user is authorised, the Italian network generates a temporary record for the user in the Italian VLR 46.

As described above, there are problems associated with roaming services in that users connected to a roamed-to network incur heavy surcharges when making or receiving calls or using data services on their mobile phones. This is true regardless of where the user is calling, or who is calling the user. In the above example, the user visiting Italy will incur roaming charges when calling local Italian phone numbers as well as calling phones in the home network in the UK and elsewhere. Similarly, roaming charges will be applied to incoming calls from either UK, Italian or other phone numbers.

The prior art methods for reducing these roaming charges are cumbersome as they require the user to purchase, carry around, and maintain the accounts of, many different SIM cards, or they require a high degree of user interaction in order to utilise one of the services to circumvent these roaming charges. However, as described above there are many known
5 problems with these services.

As described above, WO 2011/036484, the disclosure of which is incorporated by reference herein to the extent permitted by law, provides an additional central server within a typical cellular telecommunications network. The additional central server is able to provide, as
10 required, a plurality of additional IMSIs to a mobile phone, when the mobile phone is connected to a roamed-to network in another country/region. The additional central server is referred to as an IMSI Broker. In such a system, the IMSI Broker is arranged to determine whether the SIM card in the mobile phone has an appropriate IMSI for the roamed-to network. The SIM cards required for this embodiment of the invention are capable of storing
15 a plurality of alternative IMSIs for different networks, together with associated rules governing when the alternative IMSIs should be used. In this embodiment, the IMSI broker has access to a database store of alternative (new) IMSIs for multiple foreign networks (FNOs) and is arranged to distribute these new IMSIs as necessary to users who are subscribed to a network comprising an IMSI broker and, who are roaming across networks.

20 In this arrangement, each SIM has the capability of storing a plurality of IMSIs that can be used in a specific territory (country or region) to achieve the best possible calling rates. The SIM also has a set of rules to drive the selection of the best possible IMSI. Every time a user enters a different territory (mostly a new country, but it could also be a new region within a
25 country), the IMSI Broker will issue the best possible IMSI and IMSI selection rules for that territory. The IMSI Broker will send this new IMSI to the SIM via Over The Air (OTA). This solution eliminates the need to swap out SIMs when new wholesale network deals become available. Subscribers are issued an additional IMSI when and where available.

30 Updates and management of the data in the SIM can be achieved over the air interface using any available OTA radio connection. Some examples, include but are not limited to, cellular signalling channels, cellular data connections, text messaging, WiFi, Bluetooth & WiMAX. A person skilled in the art will appreciate that 'OTA' shall include all possible connections to the mobile handset and any other method of transferring data to the handset
35 device such as wired connection to a PC, Infra-Red and so on.

Using this approach, the SIM may, at the time of manufacture, be programmed to include a plurality of IMSIs corresponding to popular destinations. In another embodiment, the SIM may be programmed with a plurality of IMSIs at registration with the network, in accordance with user selection of countries or territories to which the user expects to visit in the future. In another embodiment, the SIM may only comprise one IMSI after manufacture and registration, such that all of the new/alternative IMSIs are delivered from the IMSI Broker as and when the user visits new countries/territories.

SIMs are evolving continuously, and currently known SIMs may be capable of storing up to 256 different IMSIs in the SIM's memory. This number is likely to increase further. However, regardless of the number of IMSIs that the SIM is able to hold, other memory constraints may mean that an upper limit is placed on the number of IMSIs to be stored within the SIM. In cases where an upper limit is reached, according to one embodiment of the present invention, the SIM is able to dynamically overwrite a stored IMSI with a newly obtained IMSI. The decision as to which IMSI is overwritten can be based on a number of factors, for example, any unused IMSI may be the first to be overwritten. Likewise IMSIs that have been used the least, or which have been used less frequently may be overwritten before more popular/recently used IMSIs.

While embodiments of the present invention may be used effectively with the IMSI Broker described here, and in more detail in WO 2011/036484, the IMSI Broker is not itself an aspect or feature of the present invention, which is directed to management of identity at a mobile device.

Figure 2 shows a schematic overview of an integrated IMSI Broker 108 and a handset SIM 530 in communication with it over a network. In this sense, network need not be limited to the physical network which is operated by a single network operator. In other words, the term network may be taken to mean a collection of co-existing networks.

The MSC of a network communicates with the HLR 111, which in turn communicates with the IMSI Broker 108 and an Intelligent Network (IN) / Back-office Services system (BSS) module 113. The IN/BSS module has access to a user dB which comprises a record for each user subscribed to the network. The IN/BSS module 113 is responsible for monitoring the user's usage, i.e. voice calls, SMSs, data usage etc, such that a record is kept for billing purposes. In one embodiment, the IN module 113 is also responsible for ensuring that caller ID information, also known as Caller Line Identification (CLI), is stored and provided during calls while roaming, to ensure that there is transparency for the called parties.

The IMSI Broker 108 has access to an IMSI Pool 109, which is a database comprising a plurality of available IMSIs for different territories/locations. IMSIs by their nature are territory specific. They are both country specific, and may also be region specific in countries (i.e. USA, India) where there may be surcharges for regional roaming as well as international roaming. An IMSI which is registered on an HLR in one territory will be deemed to be roaming if connected to a network/HLR in a different territory. Therefore, for each territory in the IMSI Pool 109 there is a sub-pool or range of suitable IMSIs which may be used. This is described in more detail later.

The IMSI Broker 108 comprises an IMSI updater 500, and IMSI checker 510, and a rules manager 520.

The network also comprises an OTA module which is arranged to send update messages to mobile phones as necessary. The update messages may include alternative IMSIs and/or rule update messages. This updating mechanism is not limited to provision of alternative IMSIs or associated rules – it may also be used to provide other updates to the SIM card (such as new versions of installed software) and also for verification of settings.

The HLR is further arranged to communicate with a plurality of foreign networks (operated by foreign network operators FNOs). The communication channel between the HLR and foreign networks is through the SS7 network.

Figure 2 also comprises a schematic block diagram of the functional components within the SIM 530. As shown the SIM comprises a current IMSI 540, a current MSISDN 542, a SIM application (SIMAPP) 544 for executing functional steps on the SIM, and a database 546 of available IMSIs, associated rules, and MSISDNs.

The skilled person will review WO 2011/036484 for further details of the IMSI Broker system, as required. Embodiments of the present invention will now be described with reference to a SIM of the type illustrated in Figure 2 – as indicated above, such a SIM may or may not be used in connection with an IMSI Broker system as indicated here, or may be used independently of such a system (or with a different type of system for providing user identities where required).

In one aspect, aspects of the invention involve a method of managing identities for use in a mobile telecommunications device in a telecommunications network, the method comprising:

triggering an identity management process;
 detecting one or more parameters associated with the mobile telecommunications device;

in the identity management process, selecting an identity management rule
 5 determined by the one or more parameters detected;

in the identity management process, searching an identity database wherein each record comprises an identity and additional identity information for each identity, wherein the searching prioritises records according to the identity management rule;

10 in the identity management process, selecting an identity when a record conforming to the identity management rule is found in said searching; and

in the identity management process, modifying an active identity of the mobile telecommunications device to be the selected identity when the active identity is not already the selected identity.

15 This approach can be used on different types of telecommunications network, but is effective on a GSM network, or on a 3G or LTE network as specified by 3GPP. The SIM may be a conventional SIM, or may be a USIM running on a smart card running on a 3G phone – the term “SIM” will be used hereafter for all types of SIM, whether embodied as a SIM card, an application on a smart card, or a routine instantiated virtually. Advantageously, such a SIM is
 20 designed and implemented according to currently applicable standards (at the present time, such standards include ETSI TS 151.011, ETSI TS 131 101, ETSI TS 102 221, ETSI TS 131 102, ETSI TS 131 111 and ETSI TS 151 014). An effective approach for implementing the method to be described is a USIM and SIM combination in which the SIM and USIM
 (hereafter called (U)SIM) are designed and implemented as per ETSI TS 151.011, ETSI TS
 25 131 101, ETSI TS 102 221, ETSI TS 131 102, ETSI TS 131 111 and ETSI TS 151 014. Additionally, an application and additional files are added to the (U)SIM that implement the method.

As shown in Figure 3, there are a series of main stages are present in a process operated according to an embodiment of the invention. These are a trigger step 1, an identity selection
 30 step 2, a pooling identity selection step 3, and an identity swap step 4, 5. The identity selected and swapped is in this case an IMSI – the approach shown here may however be applied to the selection and swapping of other identity types. Also described below, though not shown in Figure 3, is a mechanism for making status queries.

35 Figure 4 illustrates different possible trigger steps and their consequences. In embodiments, any of the following events can trigger further operation of the application:

- The (U)SIM coming out of RESET
- A SIM or card application toolkit profile download received by the (U)SIM.
- A SIM or card application toolkit EVENT(Location Status)
- A change to the contents of any specific UICC file.
- 5 • A STATUS command is received by the (U)SIM.
- A specific plugin is called in the WIB environment.
- By a specific message over a Java shareable interface.
- A change to the IMSI storage file used by the application by a message from a remote service (IMSI Broker).
- 10 • An instruction to change IMSI to a specific IMSI from a remote service (IMSI Broker).
- An instruction to change the IMSI selection mode to 'AUTOMATIC' from a remote service.

If the trigger is the (U)SIM coming out of RESET then the application shall initialise itself. As part of this initialisation the SIM may either remove all networks from the forbidden list
 15 (defined in ETSI TS 151 011 and ETSI TS 102 221) or remove just the preferred network for the current known location before the handset reads this file. Optionally if the IMSI selection mode is set to 'MANUAL' then the IMSI selection mode may be changed to 'AUTOMATIC'.

If the trigger is the (U) SIM receiving a SIM or card application toolkit profile download then the application shall analyse the contents of the profile download to determine the level of
 20 support the handset has for different aspects of the application function. If the handset supports the SIM or Card application toolkit EVENT(Location Status) then it shall use incoming events to automatically trigger IMSI changes, and otherwise it shall monitor changes in the (U)SIM files and STATUS commands to trigger IMSI changes. OTA triggers and triggers from other applications on the card (such as the WIB or Java applications) shall
 25 always be available regardless of the TERMINAL PROFILE.

If the trigger is a SIM or card application toolkit EVENT(Location Status) then the application shall the application shall use the PROVIDE LOCAL INFORMATION (cell id) to determine the network connection status and the MCC and MNC of the current network (if available) and then follow the IMSI selection procedure.

30 If the trigger is a change to any specific file being monitored for this purpose then following the file change the application shall use the PROVIDE LOCAL INFORMATION (cell id) to determine the network connection status and the MCC and MNC of the current network (if available) and then shall follow the IMSI selection procedure.

If the trigger is a STATUS command is received by the (U)SIM then the application shall decide whether this STATUS command shall be used as a trigger. This may be decided based on the number of STATUS commands received or by some other means. If triggered by the STATUS command, the application shall use the PROVIDE LOCAL INFORMATION (cell id) to determine the network connection status and the MCC and MNC of the current network (if available). It will then follow the IMSI selection procedure.

If the trigger is a change to the IMSI storage file used by the application or due to a WIB plugin call with the trigger type set to automatic, or due to a communication with a Java application over a shareable interface where the selection mode is set to automatic, or a message from a remote service (IMSI Broker) to go into 'AUTOMATIC' mode, then the application shall use the PROVIDE LOCAL INFORMATION (cell id) to determine the network connection status and the MCC and MNC of the current network (if available). It will set the IMSI selection mode to 'AUTOMATIC' and then follow the IMSI selection procedure.

If the trigger is the selection of a specific IMSI either due to a WIB plugin call with the trigger type set to manual or due to a communication with a Java application over a shareable interface where the selection mode is set to manual or due a message from a remote service (IMSI Broker) then the IMSI selection mode shall be set to 'MANUAL' and the IMSI swap process shall be followed using the specified IMSI.

The IMSI selection procedure will now be described. The procedure described below in detail is the automatic process, but there is also an option to bypass the automatic process by allowing manual selection.

The automatic IMSI selection process is a 2 step procedure:

- Step 1 (shown in Figure 5) – Selection of an IMSI based on a specific action based on the type of handset and network detected
- Step 2 (shown in Figure 6) – Selection of an IMSI based a set criteria from a pool of IMSIs available for this purpose (pooling). This selection is not based on the current network.

On entry to the IMSI selection procedure, if the IMSI selection mode is set to manual then the method ends with no change.

If the IMSI selection mode is set to automatic then the handset IMEI is detected, the subscription type is read from the SIM and the MCC and MNC is retrieved from the result of a PROVIDE LOCAL INFORMATION – Cell ID SIM toolkit Command. This process is

described below in more detail with reference to Figure 5. It comprises two main stages: determination of the subscription type, and determination of the IMSI to use based on subscription type and network code.

The process is started by a specific action (step 1001), for example as discussed above with regard to triggering steps. The IMEI (International Mobile Equipment Identity, providing a unique identity for each mobile device) for the device is then retrieved (step 1002), and the TAC code retrieved (the TAC or Type Allocation Code identifies the model and origin of the device and is provided as an 8-digit number forming part of the IMEI).

The TAC code is then matched to a record stored in the SIM (steps 1003 and 1004). This need not be an exact match – a wild card mechanism may be used to match only part of the TAC code. If a record is found (step 1006) then the actual subscription type to be used and the swap mechanism to be used is determined from that record by using the initial subscription type from the SIM. As discussed below, the swap mechanism is also made dependent on parameters of the device itself. If no specific IMEI TAC is matched (step 1005) then a record marked as a default entry may be used - the actual subscription type to be used and the swap mechanism to be used is then determined from that record by using the initial subscription type from the SIM. If no default entry exists for the IMEI matching then the subscription type is unmodified and the swap mechanism to be used shall be the default swap mechanism set by the method.

Like handset type, subscription type is also a property of the mobile device itself. In some cases, this will be determined by the operating system and processes of the device itself (for example, Apple and BlackBerry devices are differentiated in this way). It may also be determined by whether the device is operating according to a prepaid or a postpay protocol, or by whether the device is configured for voice, data, or a combination of the two.

Once the handset type and subscription type have been established, this is used for IMSI selection. Firstly, a currently active network is determined (step 1007) and an attempt is made to match the MCC/MNC combination of the current network to a record stored in the SIM (step 1008). As described previously for the IMEI/TAC, a wild card mechanism may be used to match only part of the MCC/MNC code.

If a record is found (step 1009) then the IMSI to be used (or a reference to that IMSI) is determined by using the IMSI assigned for the current subscription (step 1010). This will typically be a unique choice already determined for that description. After the selection, the IMSI swap process is initiated (step 1011) as is described further below. However, if no

entry exists for the MCC/MNC code matching (step 1012) then a pooling mechanism is used to provide an appropriate IMSI. This is discussed with reference to Figure 6.

The pooling process indicated in Figure 6 relies on the handset type and subscription being known as discussed above – the handset type and subscription constrain the choices

5 available in the pooling process to those which are suitable for that handset and subscription. The process is called if there is no match to a specific MCC/MNC.

There are many mechanisms specified for IMSI pooling and further methods can be added remotely over the air. The selection of the pooling mechanism to use may be stored on the SIM, or may be provided as an input to the process through the trigger.

10 In the embodiment described here, the following mechanisms may be supported:

- Use first entry – always use the IMSI based on the subscription type for the first entry in the pooling list.
- Match first occurrence of MCC – use the IMSI indicated based on the subscription type for the first pooling record that contains the current MCC else use first record.
- 15 • In rotation - use the IMSI indicated based on the subscription type for the next pooling record from the pooling record used prior to the last switch on.
- Random - use the IMSI indicated based on the subscription type for the randomly selected pooling record chosen at switch on.
- External application – one or more external application is called to make the IMSI
20 selection.

The implementation of these choices and the resulting process is shown in Figure 6.

If the new IMSI is different from the current IMSI then the IMSI swap process is followed.

If the new IMSI is the same as the current IMSI and if the current IMSI is not allowed to connect to the “allowed network” for that IMSI (this may be indicated as a “limited service”
25 response to a PROVIDE LOCAL INFORMATION(Cell ID) command, a “limited service” indication in the EVENT(Location Status) or a “PLMN not allowed or “Routing area not allowed” in any Loci file.) then the recover service process indicate below is followed.

If the SIM is in “network backup mode” the MCC indicated is the same as the previous MCC indicated then the recover service process is followed. However, if the SIM is in “network
30 backup mode” the MCC indicated is different to the previous MCC indicated then the “network backup mode” is cleared.

The network recover service is used when the expected service is not available. This feature, which is an option which may be disabled without affecting the operation of other features of this embodiment, is used to try and deliver service to a user when the automatically chosen IMSI is forbidden on a network that the SIM expects service. The

5 recover service process checks if a backup IMSI value indicated for the current record is the same as the current IMSI. If it is not the same, the IMSI will be changed using the IMSI change procedure. The SIM shall then set "network backup mode" as being in effect.

The manual selection process may be chosen as an alternative to the automatic process, and may be triggered, for example, by a WIB plugin, a java applet via the shareable interface
10 or by an OTA update of the EF manual IMSI file.

Using this approach, If the IMSI value indicated manually is different to the current IMSI then the application checks the IMEI of the device and matches it to a record in EF IMEI_Specific_Info. The indicated IMSI swap mechanism for that IMEI (or the default record if there is no match) stored on the SIM is then used to change the IMSI.

15 Returning to Figure 3, the Change IMSI process to allow IMSIs to be swapped is carried out as follows.

On entry into the IMSI swap procedure the application first checks whether the new IMSI to be selected is the same as the existing IMSI being used.

20

If it is the same, then the application exits without making any change to the IMSI and its associated parameters.

If it is different, then the Change IMSI procedure is actioned. This process is started if the
25 SIM determines it needs to change IMSI. The IMSI swap process is based on the handset type and its associated entry in the record for that handset type.

The following processes may be supported, for example:

- Refresh (type 6) with all change files notified
- 30 • Refresh (type x) where x is passed to the routine
- Display to user asking them to switch the phone off then on again
- through a separate application 1
- through a separate application 2

The particular process to be followed may be determined for a specific handset type chosen to be in accordance with the handset capabilities in order to ensure effective function.

The application uses the card application toolkit REFRESH command to reset the GSM/3G/LTE session and to inform the handset that the following files have changed. If the handset does not support this command an alternative approach will be taken, such as the application requesting that the user switches the handset off and on using the card application toolkit DISPLAY TEXT command. Alternatively, for particular handsets a different application entirely may be initiated.

When the UICC restarts, either due to the REFRESH or to whatever change process is used, in embodiments the application may change the following before the handset reads them:

- EF IMSI in DF GSM and ADF USIM are set to the new IMSI.
- EF SMSP is changed to the SMSC value relevant to the new IMSI (optional).
- EF OPLMNwACT is changed to the correct content relevant to the new IMSI (optional).
- The authentication parameters are set to the relevant values for the new IMSI(optional).

The EF LOCI and EF PS_LOCI in DF_GSM and ADF USIM are set to their initial provisioned value.

The modification of identity may include the modification of one or more of the following files in the SIM: EF LOCI, EF PS_LOCI, EF GPRS_LOCI, EF OPLMNwACT, EF PLMNwACT, EF HPLMNwACT, EF PLMNsel, EF FPLMN and EF HPPLMN.

Figure 7 indicates the types of record held by the SIM in the course of this process and the respective record structures. A single initial information record will indicate, for example, a subscription type and a pooling mechanism to use. Device type records may indicate, for example, modifiers to a subscription type (an initial voice and data subscription may for example need modification to indicate that the device is a BlackBerry, with its own data

handling protocols). A specific MCC record may effectively divide IMSI and PLMN lists by appropriate subscription, as may pooling records. A specific IMSI record may indicate not only the IMSI, but authentication, address and network identity information too.

- 5 The information used for these processes may be used for more than IMSI selection. The method may in embodiments include a query process that allows other applications to ask whether the current IMSI is the correct IMSI. This method may also generate an event for other applications when the correct IMSI is selected and the handset is in a stable state. This event will have a means for the receiving application to register and de-register for this
10 alert. All aspects of the process may be logged in this way.

This approach allows for reliable management of identity at a mobile handset, reliability being improved by enabling the procedure to be optimised for different handset and subscription types – while described here with reference to IMSI data, it is also applicable to
15 other types of identity for use with a communication network. This approach is also effectively used in combination with an IMSI Broker as discussed in WO 2011/036484, which can dynamically provide new identities and supporting information and parameters to a mobile handset, and which can also be a source of trigger events to prompt a change of IMSI where this is determined to be desirable.

20

The operational data contained in a database record of IMSI data may optionally contain primary data or links or pointers, optionally nested, to additional operational data contained other SIM database files.

- 25 The SIM database may optionally be pre-loaded at manufacture, or modified by OTA information sent from the host system.

The term territory used herein is intended to mean any specific locality, this may be in terms of countries, regions and possible even for given networks.

30

The terms mobile phone, handset, mobile terminal, communications device may be considered as being interchangeable within this document.

- 35 A person skilled in the art will appreciate that the present invention is not limited to details of the described embodiments, rather numerous changes and modifications may be made without departing from the spirit and scope of the invention as set out in the appended claims.

Claims

1. A method of managing identities for use in a mobile telecommunications device in a telecommunications network, the method comprising:
- 5 triggering an identity management process;
- detecting one or more parameters associated with the mobile telecommunications device;
- in the identity management process, selecting an identity management rule determined by the one or more parameters detected;
- 10 in the identity management process, searching an identity database wherein each record comprises an identity and additional identity information for each identity, wherein the searching prioritises records according to the identity management rule;
- in the identity management process, selecting an identity when a record conforming to the identity management rule is found in said searching; and
- 15 in the identity management process, modifying an active identity of the mobile telecommunications device to be the selected identity when the active identity is not already the selected identity.
2. A method as claimed in claim 1, wherein each said identity comprises an IMSI.
- 20 3. A method as claimed in claim 1 or claim 2, wherein the one or more parameters comprise a handset type.
4. A method as claimed in claim 3, wherein the handset type is determined from the
- 25 TAC code in the IMEI of the handset.
5. A method as claimed in any preceding claim, wherein the one or more parameters comprise a subscription type associated with the device, wherein the subscription type relates to one or more of a device operating system and a communication type.
- 30 6. A method as claimed in any preceding claim, wherein the additional information comprises an MCC and an MNC for each identity.
7. A method as claimed in claim 6, wherein the identity management rule allows for
- 35 selection of an identity based on matching of some or all of an MCC or an MNC value.

8. A method as claimed in claim 6 or claim 7, wherein if there is no match established by the identity management rule to a specific identity, a new identity is selected from a pool of matching identities.

9. A method as claimed in any preceding claim, wherein a process of modifying the active identity is determined according to the one or more parameters of the device.

10. A method as claimed in any preceding claim, wherein if on modifying the active identity no service is provided to the new active identity, the active identity is modified to a backup identity different from the identity for which no service was provided.

11. A subscriber identity module for use in a mobile telecommunications device and having a plurality of identities for use in a mobile telecommunications network, the subscriber identity module comprising a memory and a processor, wherein the memory comprises an identity management process for execution by the processor and an identity database, wherein the processor is adapted to:

on triggering, initiate the identity management process;

detect one or more parameters associated with the mobile telecommunications device;

in the identity management process, selecting an identity management rule determined by the one or more parameters detected;

in the identity management process, search an identity database wherein each record comprises an identity and additional identity information for each identity, wherein the searching prioritises records according to the identity management rule;

in the identity management process, select an identity when a record conforming to the identity management rule is found in said searching; and

in the identity management process, modify an active identity of the mobile telecommunications device to be the selected identity when the active identity is not already the selected identity.

12. A subscriber identity module as claimed in claim 11, wherein each of the plurality of identities are IMSIs.

13. A subscriber identity module as claimed in claim 11 or claim 12, wherein the one or more parameters comprise a handset type.

14. A subscriber identity module as claimed in claim 13, wherein the handset type is determined from the TAC code in the IMEI of the handset.

15. A subscriber identity module as claimed in any of claims 11 to 14, wherein the one or more parameters comprise a subscription type associated with the device, wherein the subscription type relates to one or more of a device operating system and a communication type.

16. A subscriber identity module as claimed in any of claims 11 to 15, wherein the additional information comprises an MCC and an MNC for each identity.

17. A subscriber identity module as claimed in claim 16, wherein the identity management rule allows for selection of an identity based on matching of some or all of an MCC or an MNC value.

18. A subscriber identity module as claimed in claim 16 or claim 17, wherein if there is no match established by the identity management rule to a specific identity, a new identity is selected from a pool of matching identities.

19. A subscriber identity module as claimed in any of claims 11 to 18, wherein a process of modifying the active identity is determined according to the one or more parameters of the device.

20. A subscriber identity module as claimed in any of claims 11 to 19, wherein if on modifying the active identity no service is provided to the new active identity, the active identity is modified to a backup identity different from the identity for which no service was provided.