

METHOD AND SYSTEM FOR CHANGING OVER SMARTCARDS

FIELD OF INVENTION

The present invention relates broadly to changing over smartcards. As an example, the present invention is described by the changing over of a Subscriber Identity Module (SIM) card to another SIM card on a mobile phone device.

BACKGROUND

There are a few instances a smartcard needs to be exchanged. For example, when a new application is developed on a SIM card, or when users decide to upgrade the SIM cards (eg. to a card with bigger memory space), or when users decide to change a telco operator or service provider.

In the case of the SIM card, when such need arises, the current practice is that subscribers have to travel down to the nearest Point Of Sale (POS) to carry out the exchange. POS usually refers to shops where mobile phones and subscriptions are sold. This is a big hassle for users as it takes up their personal time and incurs cost. Furthermore, there will be a period of transition where the subscriber will not be able to make or receive any calls. Furthermore, inconvenience usually results from e.g. transferring the Abbreviated Dialling Number (ADN) list on the old SIM card to the new SIM card. ADN list or simply called the phonebook refers to the speed dial numbers that can be programmed into the SIM card memory. In addition, this practice is also an inconvenience for telco operators as logistic arrangements have to be made to distribute the SIM card to the various POS location. This again incurs time and cost.

The current practice of SIM card exchange as mentioned creates a certain level of dissatisfaction for the subscribers and thus inhibits telco operators from actively exchanging SIM cards for the majority of their subscribers. Moreover, SIM card exchange of large scale will require additional staff at the outlet and may impact other activities in the shops. As such, another practice should be adopted.

One such practice would be to post the SIM card to the cardholder using registered or normal mail. However, this is not accepted by the telco operators because of a few concerns.

Firstly, telco operators cannot track the exact receipt time of the new card and are hence unable to coordinate the change over to the new card.

Secondly, there are security concerns as a new card may be lost, mis-used or tampered with during transportation, and confirming that a new card is indeed used by the targeted subscriber.

Hence, it was with knowledge of the foregoing concerns that the present invention was conceived and has now been reduced to practice.

SUMMARY

In accordance with a first aspect of the present invention there is provided a method for remotely changing over smartcards comprising the steps of receiving at a central location a request for changing over smartcards from a user of a remote device utilising a first smartcard; comparing the request with a database of anticipated requests; and providing a key to the user for accessing a second smartcard.

The request may comprise a first portion input by the user and a second portion inherently associated with the first smartcard.

The second portion of the request may comprise one or more of a group comprising a Mobile Station Integrated Services Digital Network number (MSISDN), an International Mobile Subscriber Identity (IMSI) and an Integrated Circuit(s) Card Identifier (ICCID).

The method may further comprise the step of the user gaining access to the second smartcard utilising the key.

The method may comprise verifying the key using an anticipated key pre-stored on the second smartcard.

The anticipated key and/or the provided key may be encrypted.

The provided key may unlock a PIN of the second smartcard for gaining access.

The method may further comprise setting permanently a seal code to indicate that the second smartcard has been accessed at least once.

A message may be automatically sent from the remote device to the central location to indicate the second smartcard is ready to be activated for use in a communication network.

The method may further comprise automatically connecting the second smartcard to the network of a service provider at the central location to activate the smartcard according to the protocol standards of a mobile communication network service provided by the service provider.

The method may further comprise the step of automatically transferring data of the first smartcard previously downloaded at the central location to the second smartcard.

In accordance with a second aspect of the present invention there is provided a system for remotely changing over smartcards comprising a central server for receiving a request for changing over smartcards from a user of a remote device utilising a first smartcard; a database for storing anticipated requests; wherein the central server compares the request with the anticipated requests in the database; and provides a key to the user for accessing a second smartcard.

The request may comprise a first portion input by the user and a second portion inherently associated with the first smartcard.

The second portion of the request may comprise one or more of a group comprising a Mobile Station Integrated Services Digital Network number (MSISDN), an International Mobile Subscriber Identity (IMSI) and an Integrated Circuit(s) Card Identifier (ICCID).

The system may further comprise the second smartcard.

The second smartcard may verify the key using an anticipated key pre-stored on a database of the second smartcard.

The anticipated key and/or the provided key may be encrypted.

The the provided key may unlock a PIN of the second smartcard for gaining access.

The second smartcard may set permanently a seal code of the second smartcard to indicate that the second smartcard has been accessed for at least once.

The second smartcard may initiate sending a message from the remote device to the central server to indicate the second smartcard is ready to be activated for use in a communication network.

The central server may initiate connecting the second smartcard to the network of a service provider to activate the smartcard according to the protocol

standards of a mobile communication network service provided by the service provider.

The central server may transfer data of the first smartcard to the second smartcard.

In accordance with a third aspect of the present invention there is provided a smartcard comprising a PIN to be unlocked by a key so as to allow access to the smartcard; a database for storing an anticipated key; a processing unit for verifying the integrity of the key by comparing the key with the database; and a seal code for indicating that the smartcard is used for the first time.

The seal code may comprises a file in the Master File Directory of the smartcard.

The file may comprise a validity field that is deemed valid when the smartcard is accessed for the first time and deemed invalid when the smartcard is accessed for more than one time.

The processing unit may check the validity field of the seal code every time a user keys in the key.

The PIN may be unlocked for the user to gain access to the smartcard after the processing unit verifies that both the key is correct and the validity field is valid.

The key and/or the anticipated key me be encrypted.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only and in conjunction with the drawings, in which:

FIG. 1 is a schematic view of the example embodiment.

FIG. 2 is a flowchart showing the steps of changing over the SIM cards of the example embodiment.

FIG. 3 is a flowchart detailing the steps of breaking seal of the new SIM card on the mobile device of the example embodiment.

FIG. 4 is a table tabulating the properties of the software patch file to the SIM card command table of the example embodiment.

DETAILED DESCRIPTION

In detail, FIG. 1 shows the hardware setup of an example embodiment that is used to describe the present invention.

The hardware setup comprises a remote server (150), a remote mobile device (130), a SIM card slot (120), an old SIM card (100), a new personalised SIM card (110) and a wireless connection (140).

The remote server (150) is a device residing in the mobile network of telco operators or service providers. It comprises processing, data storage, wireless data transmission and wireless data receive capabilities. The remote server (150) is used to verify the identity of the targeted subscriber and to provide the subscriber with a one time usage Sealed PIN Unblocking Key (SealPUK) where PIN stands for Personal Identification Number.

The remote mobile device (130) is a device residing in a remote location with the subscriber. It comprises processing, data storage, wireless data transmission, and wireless data receive capabilities. The remote mobile device (130) houses a SIM card in its SIM card slot (120).

The SIM card slot (120) is a slot on the mobile device used to house the SIM card and to connect the SIM card that is slotted in it to the remote mobile device (130).

The old SIM card (100) is a SIM card that the subscriber wants to replace.

The new personalised SIM card (110) is a SIM card that the subscriber wants to use to replace the old SIM card (100). Having gone through a personalisation process, it comprises a root directory, a Mobile network system (eg. GSM - Global System for Mobile communications) directory, and a Telco operator directory. The datafields of these directories contain information of the electronic profile supplied by the subscriber. For a typical GSM system, examples of essential information contained in the electronic profile are International Mobile Subscriber Identity (IMSI), Integrated Circuit(s) Card Identifier (ICCID), Subscriber Authentication Key (Ki), Card Holder Verification information (CHV) and code for unblocking the specific CHV (UNBLOCK CHV). During the personalisation process, SIM applications are also downloaded into the SIM card.

It is to be noted that for the example embodiment, the instructions in the operating system of the SIM card and the files in the directories have been adjusted

to accommodate a subscriber verification process. Such adjustments can be made during personalisation or during manufacturing the card. The purpose of the adjustments is to create a software feature referred to herein as SIMSeal in the new personalised SIM card (110). SIMSeal is the virgin status of a SIM card. It is only noticeable to the first user. Once the seal is broken, SIMSeal cannot be restored, and hence it can be used to indicate the SIM card has been used before. The adjustments made to enable SIMSeal are described in a later part of the detailed description.

The wireless connection (140) in this example refers to a physical communication connection between the remote mobile device (130) and the remote server (150) established by GSM standards.

For the purposes of this example, the remote mobile device (130) is located, for instance, in a Public Land Mobile Network (PLMN) and the PLMN can be a GSM system. Further, the remote mobile device (130) is located, for example, in the PLMN area of the subscriber's home operator or located within the PLMN area of other operators where roaming is agreed between the operators. The remote server (130) is connected wirelessly and/or wired to the PLMN of the subscriber's home operator and it can establish a wireless connection (140) with the remote mobile device (130).

In detail, FIG. 2 illustrates the step-by-step procedure of the example embodiment using the hardware setup of FIG. 1.

It is to be noted that all the messages sent by the subscriber using the remote mobile device (130) and sent by the remote server (150) are based on Short Message Service (SMS) in the example embodiment. For the purposes of this example, the new personalised SIM card (110) is delivered by conventional mail (registered or non-registered).

After receipt, the first step (200) is performed. With the old SIM card (100) in the SIM card slot (120) of the remote mobile device (130), the subscriber sends a message to the remote server (150). The content of the message contains an instruction from the subscriber to the remote server (150). The instruction can be "change PIN", which indicates the subscriber's intention to change over the old SIM card (100) to the new personalised SIM card (110).

In the second step (210), the remote server (150) receives the subscriber's message through the wireless connection (140). In the same receiving session, it also receives an identification code of the old SIM card (100). For example, this identification code of the old SIM card (100) can be the Mobile Station Integrated Services Digital Network number (MSISDN), International Mobile Subscriber Identity (IMSI) or Integrated Circuit(s) Card Identifier (ICCID). In the subsequent steps of the present example, MSISDN is used. It is noted that the provision of the identification code is not controlled/manipulated by the user.

In the third step (220), the remote server (150) checks whether both the message and MSISDN are correct. This check is performed to verify the identity of the targeted subscriber for a particular SIM card. Firstly, comparing the received message with the desired message pre-stored in a database residing on the remote server (150). Secondly, comparing the received MSISDN with a pre-stored value of the subscriber's MSISDN in a database residing on the remote server (150).

If the message and/or the MSISDN do not match, it means the subscriber is not the targeted subscriber. In such a case, the remote server (150) will perform actions (260) defined by the administrators of the remote server (150), for example, warning the subscriber of unauthorised access or not responding to the subscriber at all.

If both the message and MSISDN matches the data on the remote server (150), the subscriber sending the message using the remote mobile device (130) is verified to be the targeted subscriber and the fourth step (230) can be performed.

In the fourth step (230), the remote server (150) acknowledges the subscriber by sending a return message containing a SealPUK via the wireless connection (140) to the remote mobile device (130). The SealPUK is a one-time usage PIN Unblocking Key (PUK) used to break the SIMSeal.

In the fifth step (240), the subscriber receives the message containing the SealPUK from the remote server (150) on his or her remote mobile device (130). He or she then changes SIM cards by removing the old SIM card (100) from the SIM card slot (120) and inserting the new personalised SIM card (110) into the SIM card slot (120).

In the sixth step (300), the subscriber uses the SealPUK to break the SIMSeal and gain access to use the new personalised SIM card (110). This step will be discussed in greater detail later with reference to FIG. 3.

The final juncture (250) is where the subscriber has gained access to the new personalised SIM card (110). The remote mobile device (130) is now ready for activation of the new personalised SIM card (110).

After this juncture, a delivery report (for eg. a SMS message or a signal triggered by the new personalised SIM card (110)) is sent automatically from the remote mobile device (130) to the remote server (150) to indicate that the new personalised SIM card (110) is ready for activation. The remote server (150) then links up with a system residing with the service provider, such as an authentication centre (AUC) within the Operation and Maintenance Subsystem (OMSS) of the GSM PLMN. After linking up, the remote server (150) automates the change over of the identification code of the old SIM card (100) to the identification code of the new personalised SIM card (110) with the aid of the linked up system. After the changing session is complete, the new personalised SIM card (110) is activated.

Following this activation, the remote server (150) can automatically start to transfer records and applications belonging to the old SIM card (100) into the new personalised SIM card (110). It is to be noted that if this transfer is required, the remote server (150), at some point in the process of FIG. 2, downloads all the records and applications in the old SIM card (100). An example of records would be the ADN list of the old SIM card (100). An example of an application would be an electronic organiser.

Otherwise, if not done automatically by the remote server, the transfer of records and applications can be done manually. For example, a manual transfer may utilise a software application in the remote mobile device (130) or in the new personalised SIM card (110). This software application may contain features to download the records and applications of the old SIM card (100) into the memory of the remote mobile device (130) or on another device with memory and later aid in downloading the records and applications from the memory of the device into the new personalised SIM card (110).

In detail, FIG. 3 illustrates the step-by-step procedure of performing step six (300) in FIG. 2.

The first step (301) of step six (300) in FIG. 2 is powering on the remote mobile device (130) with the new personalised SIM card (110).

In the second step (302), an internal check is done by the remote mobile device (130). The check is done to see if a Personal Identification Number (PIN1) of the new personalised SIM card (110) has been purposely blocked and enabled during the personalisation process or during the card manufacturing process. At the same time, the internal check also checks the validity of the SIMSeal. It is to be noted that the blocking of PIN1 is used in the example embodiment to provide an additional security layer. This is unlike the usual case where PIN1 is unblocked and disabled in new SIM cards.

If the condition (310) after the check is such that PIN1 is not blocked and/or SIMSeal is invalid, the conclusion is that the new personalised SIM card (110) has been used or tampered with before.

In this case, if the new personalised SIM card (110) is tampered before, it is up to the subscriber to report the incident to the service provider.

If the condition (303) after the check is such that PIN1 is purposely blocked and SIMSeal is marked as valid, it means the new personalised SIM card (110) is used for the first time. As such, under the condition of the new personalised SIM card, the remote mobile device (130) will prompt the subscriber to key in the SealPUK to unblock PIN1 on the first user interface session at step (304).

In step (305), the remote mobile device (130) checks whether the SealPUK is keyed in correctly. It is to be noted that a value of SealPUK is pre-stored in the memory of the new personalised SIM card (110) as part of the electronic profile of the SIM card during the personalisation process or during manufacturing of the SIM card. This pre-stored value is used to verify the SealPUK keyed in by the subscriber. It is to be noted that this pre-stored value may be encoded, encrypted or compressed.

If the SealPUK does not match the pre-stored SealPUK value, the procedure loops back to condition (303) where PIN1 is blocked, SIMSeal is valid and the subscriber is required to unblock PIN1.

If the SealPUK matches the pre-stored value, the subscriber is prompted by the remote mobile device (130) to key in a new PIN1. In step (306), the subscriber keys in the new PIN1 for the first time. After keying in PIN1, the remote mobile device (130) prompts the subscriber to key in the new PIN1 the second time so as to confirm the new PIN1 keyed in the first time is correct.

In step (307), the subscriber keys in the new PIN1 for the second time. If the incorrect PIN1 is keyed in, the condition returns to step (306) and the remote mobile device prompts the subscriber to key in the new PIN1 for the first time again.

In step (308), if the correct PIN1 is keyed in, the new PIN1 is stored as the PIN1 to be used by the subscriber for normal usage of the remote mobile device.

In the final step (309) before the juncture (250) of FIG. 2, the SIMSeal is marked as invalid. This is necessary to indicate that the new personalised SIM card has been used.

In detail, FIG. 4 illustrates a newly created Elementary File Seal (EF_seal) (400), or simply called a seal, in the Master File (MF) Directory of the new personalised SIM card (110). EF_seal (400) is used to implement the software feature SIMSeal in the example embodiment.

The Identifier refers to the unique file identification number of the EF_seal (400) file within the file system of the new personalised SIM card (110).

The Structure of EF_seal (400) is defined as transparent, that is it is composed of a sequence of bytes.

The EF_seal (400) is Mandatory, meaning its existence is of significant importance to the workability of the new personalised SIM card (110).

The file size of EF_seal (400) is 9 Bytes where the first Byte holds the Seal Status Flag and the second to ninth Bytes hold the SealPUK (Length of 8 Bytes). Within the first Byte of the Seal Status Flag, one bit is used to indicate the validity of the SIMSeal. The second bit to eighth bit are Reserved for Future Use (RFU). The 8 Bytes binary coded SealPUK residing within EF_seal (400) is used to verify the SealPUK keyed in by the subscriber.

The update activity of the EF_seal (400) file is set as low. This is because the validity of SIMSeal is only updated once after the subscriber keys in the correct SealPUK (recall step 305 in FIG. 3) and after the new PIN1 (recall step 307 in FIG. 3) is confirmed.

The EF_seal (400) file type is Elementary File, i.e. it is composed of a header and a body.

The EF_seal (400) file resides within the MF Directory.

All functions stated under access conditions of EF_seal (400) file need to satisfy access condition CHV5 before they can be used. To satisfy access condition

CHV5, the subscriber must key in the correct SealPUK during subscriber verification described in FIG. 3.

A software patch is needed in the command table of the new personalised SIM card (110) to replace the existing UNBLOCK CHV function command. This patch is necessary for the new personalised SIM card (110) to display the behaviour as illustrated in FIG. 2 and FIG. 3.

The patch involves checking EF_seal (400) each time UNBLOCK CHV1 Application Protocol Data Units (APDU) command is invoked. UNBLOCK CHV1 APDU command is called upon on every attempt the subscriber keys in SealPUK on the remote mobile device (130). The subscriber has unlimited attempts in the example embodiment.

The checking of EF_seal (400) is done on the least significant bit (LSB) of the Seal Status Flag. The LSB of the Seal Status Flag also refers to the validity of the SIMSeal software feature.

If the LSB of the Seal Status Flag is 1, the conclusion is UNBLOCK CHV1 is run more than one time and SIMSeal is valid. Further, if the LSB of the Seal Status Flag is 1, the subscriber has to key in the normal PUK1 of the new personalised SIM card (110) instead of SealPUK to access the card. The usual 10 tries for PUK1 come into effect.

If the LSB of the Seal Status Flag is 0, the conclusion is UNBLOCK CHV1 is run for the first time and SIMSeal is invalid.

The patch also involves setting the LSB of the Seal Status Flag to 1 after the correct SealPUK is keyed in during the first use of the new personalised SIM card (110). First use here does not refer to the first attempt to key in SealPUK. It refers to the first correct capture of SealPUK keyed in by the subscriber during any of his unlimited attempts. It is to be noted that in other examples of the present invention, a restriction to the number of attempts for keying SealPUK can be defined. Further, it is to be noted that the LSB (as in the above example), or a defined sequence of at least one bit in the memory of the new personalised SIM card (110) can be used to indicate the validity of SIMSeal.

In the production procedure, adjustments to the random check of the cards are made in the example embodiment. For example using random check with a ratio of 3% of the total number of production cards. As PIN1 is blocked during the

personalisation process or during manufacturing the SIM card in the example embodiment, it is necessary to unblock PIN1 to check for functionality that is, SealPUK is used to break the seal. Since the read/update EF_seal (400) is protected by access condition CHV5, the Seal Status Flag can be manipulated by acquiring PIN5 and use it to reproduce the seal after checking the functionality. In order to do this, the following procedures is followed.

Firstly, production to generate the ICCID-CHV5 list into a file.

Secondly, unblock PIN1 of the test sample and performing checking of functionality.

Thirdly, after testing, a PC software is used to read from the card to get ICCID and to seek the corresponding CHV5 from the file, so as to use it to enable updating of the Seal Status Flag.

Lastly, reproduce the seal by blocking PIN1.

In the foregoing manner, a method for changing over smartcards is disclosed. Only several embodiments are described. However, it will be apparent to one skilled in the art in view of this disclosure that numerous changes and/or modifications may be made without departing from the scope of the invention.

For example, it will be appreciated that the present is not limited to application for SIM cards, but applies generally to smartcards.

CLAIMS

1. A method for remotely changing over smartcards comprising the steps of;
receiving at a central location a request for changing over smartcards from a user of a remote device utilising a first smartcard;
comparing the request with a database of anticipated requests; and
providing a key to the user for accessing a second smartcard.
2. The method as claimed in claim 1, wherein the request comprises a first portion input by the user and a second portion inherently associated with the first smartcard.
3. The method as claimed in claim 2, wherein the second portion of the request comprises one or more of a group comprising a Mobile Station Integrated Services Digital Network number (MSISDN), an International Mobile Subscriber Identity (IMSI) and an Integrated Circuit(s) Card Identifier (ICCID).
4. The method as claimed in any one of the preceding claims, wherein the method further comprises the step of the user gaining access to the second smartcard utilising the key.
5. The method as claimed in claim 4, wherein the method comprises verifying the key using an anticipated key pre-stored on the second smartcard.
6. The method as claimed in claim 5, wherein the anticipated key and/or the provided key are encrypted.
7. The method as claimed in any one of claims 4 to 6, wherein the provided key unlocks a PIN of the second smartcard for gaining access.
8. The method as claimed in claim 7, further comprising setting permanently a seal code to indicate that the second smartcard has been accessed at least once.

9. The method as claimed in any one of claims 4 to 8, wherein a message is automatically sent from the remote device to the central location to indicate the second smartcard is ready to be activated for use in a communication network.
10. The method as claimed in claim 9, further comprising; automatically connecting the second smartcard to the network of a service provider at the central location to activate the smartcard according to the protocol standards of a mobile communication network service provided by the service provider.
11. The method as claimed in any one of the preceding claims further comprising the step of automatically transferring data of the first smartcard previously downloaded at the central location to the second smartcard.
12. A system for remotely changing over smartcards comprising;
 - a central server for receiving a request for changing over smartcards from a user of a remote device utilising a first smartcard;
 - a database for storing anticipated requests; wherein
 - the central server compares the request with the anticipated requests in the database; and
 - provides a key to the user for accessing a second smartcard.
13. The system as claimed in claim 12, wherein the request comprises a first portion input by the user and a second portion inherently associated with the first smartcard.
14. The system as claimed in claim 13, wherein the second portion of the request comprises one or more of a group comprising a Mobile Station Integrated Services Digital Network number (MSISDN), an International Mobile Subscriber Identity (IMSI) and an Integrated Circuit(s) Card Identifier (ICCID).

15. The system as claimed in any one of claims 12 to 14, wherein the system further comprises the second smartcard.
16. The system as claimed in claim 15, wherein the second smartcard verifies the key using an anticipated key pre-stored on a database of the second smartcard.
17. The system as claimed in claim 16, wherein the anticipated key and/or the provided key are encrypted.
18. The system as claimed in any one of claims 15 to 17, wherein the provided key unlocks a PIN of the second smartcard for gaining access.
19. The system as claimed in claim 18, wherein the second smartcard sets permanently a seal code of the second smartcard to indicate that the second smartcard has been accessed for at least once.
20. The system as claimed in any one of claims 15 to 19, wherein the second smartcard initiates sending a message from the remote device to the central server to indicate the second smartcard is ready to be activated for use in a communication network.
21. The system as claimed in claim 20, wherein the central server initiates connecting the second smartcard to the network of a service provider to activate the smartcard according to the protocol standards of a mobile communication network service provided by the service provider.
22. The system as claimed in any one of claims 15 to 21, wherein the central server transfers data of the first smartcard to the second smartcard.
23. A smartcard comprising;
a PIN to be unlocked by a key so as to allow access to the smartcard;
a database for storing an anticipated key;

a processing unit for verifying the integrity of the key by comparing the key with the database; and

a seal code for indicating that the smartcard is used for the first time.

24. The smartcard as claimed in claim 23, wherein the seal code comprises a file in the Master File Directory of the smartcard.

25. The smartcard as claimed in claim 24, wherein the file comprises a validity field that is deemed valid when the smartcard is accessed for the first time and deemed invalid when the smartcard is accessed for more than one time.

26. The smartcard as claimed in claim 25, wherein the processing unit checks the validity field of the seal code every time a user keys in the key.

27. The smartcard as claimed in claims 26, wherein the PIN is unlocked for the user to gain access to the smartcard after the processing unit verifies that both the key is correct and the validity field is valid.

28. The smartcard as claimed in any one of claims 23 to 27, wherein the key and/or the anticipated key are encrypted.