



US 20140024343A1

(19) **United States**

(12) **Patent Application Publication**
Bradley

(10) **Pub. No.: US 2014/0024343 A1**

(43) **Pub. Date: Jan. 23, 2014**

(54) **METHOD FOR DOWNLOADING A
SUBSCRIPTION IN AN UICC EMBEDDED IN
A TERMINAL**

(75) Inventor: **Paul Bradley**, Austin, TX (US)

(73) Assignee: **GEMALTO SA**, Meudon (FR)

(21) Appl. No.: **13/991,744**

(22) PCT Filed: **Dec. 2, 2011**

(86) PCT No.: **PCT/EP2011/071674**

§ 371 (c)(1),
(2), (4) Date: **Oct. 10, 2013**

(30) **Foreign Application Priority Data**

Dec. 6, 2010 (EP) 10306359.0

Publication Classification

(51) **Int. Cl.**
H04W 8/22 (2006.01)
H04W 12/06 (2006.01)
(52) **U.S. Cl.**
CPC **H04W 8/22** (2013.01); **H04W 12/06**
(2013.01)
USPC **455/411**

(57) **ABSTRACT**

The invention proposes a method for downloading a subscrip-
tion in an UICC embedded in a terminal, this method consist-
ing in:

- transferring an ICCID to the terminal;
- sending the ICCID over an IP link to a secure vault;
- selecting in the secure vault a subscription corresponding
to the ICCID;
- transmitting the subscription to the terminal over the IP
link;
- storing the subscription in the terminal.

METHOD FOR DOWNLOADING A SUBSCRIPTION IN AN UICC EMBEDDED IN A TERMINAL

[0001] This disclosure is a national phase of PCT/EP2011/071674, filed Dec. 2, 2011, a continuation of U.S. application Ser. No. 13/312,309, filed Dec. 6, 2011, and claims priority to European Application No. 10306359.0, filed Dec. 6, 2010, the disclosures of which are hereby incorporated by reference.

[0002] The present invention concerns a method for downloading a subscription in an UICC (Universal Integrated Circuit Card) embedded in a terminal for example a mobile terminal (mobile phone) or a machine (for M2M (Machine to Machine) applications). A UICC can be in the format of a smart card, or may be in any other format such as for example but not limited to a packaged chip as described in PCT/SE2008/050380, or any other format. It can be used in mobile terminals in GSM and UMTS networks for instance. The UICC ensures network authentication, integrity and security of all kinds of personal data.

[0003] In a GSM network, the UICC contains mainly a SIM application and in a UMTS network it is the USIM application. A UICC may contain several other applications, making it possible for the same smart card to give access to both GSM and UMTS networks, and also provide storage of a phone book and other applications. It is also possible to access a GSM network using an USIM application and it is possible to access UMTS networks using a SIM application with mobile terminals prepared for this. With the UMTS release 5 and later stage network like LTE, a new application, the IP multimedia Services Identity Module (ISIM) is required for services in the IMS (IP Multimedia Subsystem). The telephone book is a separate application and not part of either subscription information module.

[0004] In a CDMA network, the UICC contains a CSIM application, in addition to 3GPP USIM and SIM applications. A card with all three features is called a removable user identity card, or R-UIM. Thus, the R-UIM card can be inserted into CDMA, GSM, or UMTS handsets, and will work in all three cases.

[0005] In 2G networks, the SIM card and SIM application were bound together, so that "SIM card" could mean the physical card, or any physical card with the SIM application.

[0006] The UICC smart card consists of a CPU, ROM, RAM, EEPROM and I/O circuits. Early versions consisted of the whole full-size (85x54 mm, ISO/IEC 7810 ID-1) smart card. Soon the race for smaller telephones called for a smaller version of the card.

[0007] Since the card slot is standardized, a subscriber can easily move their wireless account and phone number from one handset to another. This will also transfer their phone book and text messages. Similarly, usually a subscriber can change carriers by inserting a new carrier's UICC card into their existing handset. However, it is not always possible because some carriers (e.g. in U.S.) SIM-LOCK the phones that they sell, thus preventing competitor carriers' cards being used.

[0008] The integration of the ETSI framework and the Application management framework of Global Platform is standardized in the UICC configuration.

[0009] UICCs are standardized by 3GPP and ETSI.

[0010] A UICC can normally be removed from a mobile terminal, for example when the user wants to change his mobile terminal. After having inserted his UICC in his new

terminal, the user will still have access to his applications, contacts and credentials (network operator). It is also known to solder or weld the UICC in a terminal, in order to get it dependent of this terminal. This is done in M2M (Machine to Machine) applications. The same objective is reached when a chip (a secure element) containing the SIM or USIM applications and files is contained in the terminal. The chip is for example soldered to the mother-board of the terminal or machine and constitutes an e-UICC.

[0011] The present invention applies to such soldered UICCs (e-UICCs) or to such chips containing the same applications than the chips comprised in UICCs. A parallel can be done for UICCs that are not totally linked to devices but that are removable with difficulty because they are not intended to be removed, located in terminals that are distant or deeply integrated in machines. A special form factor of the UICC (very small for example and therefore not easy to handle) can also be a reason to consider it as in fact integrated in a terminal. The same applies when a UICC is integrated in a machine that is not intended to be opened.

[0012] In the next description, welded UICCs or chips containing or designed to contain the same applications than UICCs will generally be called embedded UICCs or embedded secure elements (in contrast to removable UICCs or removable secure elements). This will also apply to UICCs or secure elements that are removable with difficulty.

[0013] The present invention concerns embedded UICCs (not removable). In a first embodiment, the invention is about a method using NFC to select and download an embedded (U)SIM application (or generally speaking a complete UICC application) to a terminal comprising such an embedded secure UICC. The terminal is for example a mobile phone.

[0014] In a second embodiment, the invention is about a method using a barcode for identifying a (U)SIM application (or generally speaking a complete UICC application) to be downloaded to a terminal able to take a photograph of this barcode.

[0015] As already explained in the introduction, in the future, when there are soft SIMs or embedded SIMs inside devices, it will be necessary to select the appropriate subscription information to download to the device. The user experience could be improved by giving a single-use NFC tag identifying the subscription for the device to download.

[0016] Said otherwise, in a world where the subscription information is no longer stored in a secure removable format such as today's UICC and instead stored as a "soft SIM" or soldered secure element (e.g. a VQFN8/DFN8 secure element) then there is a need to select the correct subscription to download to the device.

[0017] The invention proposes a method for downloading a subscription in an UICC embedded in a terminal, this method consisting in:

- [0018]** transferring an ICCID to the terminal;
- [0019]** sending the ICCID over an IP link to a secure vault;
- [0020]** selecting in the secure vault a subscription corresponding to the ICCID;
- [0021]** transmitting the subscription to the terminal over the IP link;
- [0022]** storing the subscription in the terminal.

[0023] The ICCID is preferably transferred along with a ICCID's secret activation code and the secure vault verifies the pairing of the ICCID and the secret activation code before transmitting the subscription to the terminal.

[0024] In a first embodiment, the ICCID is contained in a token and the ICCID is transferred to the terminal via NFC.

[0025] The token can be constituted by a NFC tag.

[0026] In a second embodiment, the ICCID is contained in a barcode to be photographed by the terminal.

[0027] According to the first embodiment of the present invention, a NFC terminal is used.

[0028] The download of the subscription could be done through the user interface or in a push way. However, for terminals that are unlocked, a need is present (for MNO processes with legacy flows) to have a physical tag/NFC card to distribute similar to today's physical SIM card. This tag would contain a reference to the ICCID (with a security activation code known to the provisioning system and linked to an individual ICCID). Once the ICCID is submitted to the provisioning system with the correct activation code, the remote provisioning service can begin the secure transfer of the correct software (SIM profile, subscription information) for the embedded secure element.

[0029] If for example, a user has a pre-activated device X and want to buy a subscription from operator A, the flow would be as follows:

[0030] Device X is touched against NFC token Y. The token contains the ICCID and preferably also the ICCID's activation code. Device X reads the ICCID from token Y as well as (preferably) the ICCID's secret activation code which is unique (this code prevents brute-force guessing of ICCID requests to the provisioning centre).

[0031] Device X sends this ICCID over an IP link to a secure vault. The secure vault verifies the ICCID/secret activation code pairing and if valid it securely packages, encrypts and signs the entire personalisation script for the related embedded UICC (containing SIM application, USIM application, ISIM application, CSIM application, any other network authentication applications as well as any SIM application Toolkit applications and Operating System Customisations/mechanisms related to that specific MNO) as well as the relevant subscription information such as the IMSI, K, Opc, IMPU and algorithm constants. The contents of the profile would be known to the secure vault using the ICCID range or alternatively a profile code could be submitted to the system.

[0032] The secure vault transmits the above personalisation script to device X encrypted for Device X's embedded secure element (and with an anti-replay counter mechanism included) over the IP link.

[0033] Device X (including its embedded secure element) decrypts and runs the personalisation script thus provisioning the subscription onto the embedded secure element.

[0034] Device X may now access the radio network using the subscription.

[0035] In a second embodiment, the ICCID is contained in a barcode to be photographed by the terminal. After having taken a picture of the barcode, the terminal sends it to the secure vault. The secure vault then compares the received barcode with pre-registered barcodes or decodes the barcode for retrieving the ICCID. The same process as mentioned above is then undertaken.

[0036] The invention allows selection of subscription as well as profile variant remotely and makes the user experience very easy.

1. Method for downloading a subscription in an UICC embedded in a terminal, said method comprising:

- transferring an integrated circuit card identifier (ICCID) to said terminal;
- sending said ICCID over an IP link to a secure vault;
- selecting in said secure vault a subscription corresponding to said ICCID;
- transmitting said subscription to said terminal over said IP link; and
- storing said subscription in said terminal.

2. Method according to claim 1, wherein said ICCID is transferred along with an ICCID's secret activation code, and wherein said secure vault verifies the pairing of the ICCID and the secret activation code before transmitting said subscription to said terminal.

3. Method according to claim 2, wherein said ICCID is contained in a token and said ICCID is transferred to said terminal via near field communication (NFC).

4. Method according to claim 3, wherein said token is an NFC tag.

5. Method according to claim 1, wherein said ICCID is contained in a barcode to be photographed by said terminal.

* * * * *