

Description

Title of Invention: SYSTEM AND METHOD FOR SECURE CONTAINMENT OF SENSITIVE FINANCIAL INFORMATION STORED IN A MOBILE COMMUNICATION TERMINAL

Technical Field

- [1] The following description relates to securing of sensitive data in a mobile terminal.

Background Art

- [2] With the recent advancement in the mobile technology field, the size and weight of mobile terminals became dramatically reduced, thus increasing their portability and accelerating the tendency for a user to carry the mobile terminal at all times. As mobile terminals (e.g. mobile telephones and other mobile devices) are becoming more widely used, mobile terminals have steadily evolved from a mere mobile terminal with communicative functions to a terminal that incorporates various advanced functions, such as electronic mail, computer office application functions, video telephony, and more recently, mobile payment functionalities. While integrating various consumer friendly utilities into the mobile terminal may provide convenience to its user, it also raises security concerns with regard to these mobile terminals.
- [3] Security concerns associated with the greater usability of mobile terminals may be elevated by improper usage associated with misplacing, loss, theft of these mobile terminals, as well as other mishaps that may be incurred. In order to alleviate these security concerns, various techniques have been proposed for remotely locking mobile terminals to disable their functions, when mobile terminals are misplaced or stolen. With these techniques, if a mobile terminal is to be locked during a normal operating state, its functions can be disabled, thus making it possible to reduce improper usage or the theft of private information stored in the mobile terminal.
- [4] However, with the advancement of technology, the thieving population has evolved in their intelligence as well. The more educated thieves may easily break into the remotely locked mobile terminals by "jail-breaking" to retrieve sensitive information. Thus, it is no longer enough to merely lock an apparatus or application from usage, more must be done to prevent misappropriation of sensitive data stored within the mobile terminals.
- [5] Further, with the introduction of a removable secure element (SE), further complication in the security realm has been provided. As many of these SEs, which store sensitive information, may be removed before they can be locked, a simple locking security feature on these devices may not be sufficient.
- [6] A method of data deletion may be used to provide reliable security. However,

currently, the remote data deletion in the SE is limited to SEs conforming to industry standard Short Messaging Service - Point to Point (SMS-PP) protocol or Bearer Independent Protocol (BIP) (i.e. Universal Integrated Circuit Card (UICC) type SEs). In the event the device owner has a SE that does not allow access via the industry standard protocols, such as micro (secure digital) SD cards or embedded SEs (i.e. non-UICC type SEs), remote data deletion in the SE may not be feasible.

- [7] Lastly, even if sensitive stored data has been able to be deleted, there is no easy way to replace the lost data upon recovering/replacing the lost mobile terminal. Thus, even if the mobile terminal storing sensitive information is lost and then replaced, the mobile terminal must be reinstalled with all of the applications and stored data from scratch.

Disclosure of Invention

- [8] Exemplary embodiments of the present invention provide a method for securing information stored in a non-Universal Integrated Circuit Card (UICC) type secure element (SE) over-the-air (OTA). Exemplary embodiments of the present invention also provide a method for authenticating a mobile terminal with a Trusted Service Manager (TSM) and reconstructing a mobile wallet application.
- [9] Additional features of the invention will be set forth in the description which follows, and in part will be apparent from the description, or may be learned by practice of the invention.
- [10] Exemplary embodiments of the present invention provide a method for securing information OTA in a non-UICC type SE of a mobile terminal including receiving a request to initialize an OTA proxy of a mobile terminal, initializing the OTA proxy, receiving a request to secure information stored in the SE, and securing, using the OTA proxy, the information stored in the non-UICC type SE.
- [11] Exemplary embodiments of the present invention provide a method for authenticating a mobile terminal including receiving mobile terminal information and SE information from the mobile terminal; comparing the received information with stored mobile terminal information and SE information; and transmitting a command based on the comparison result.
- [12] Exemplary embodiments of the present invention provide a method for reconstructing a mobile wallet application of a mobile terminal including receiving a request to reconstruct the mobile wallet application of a user; transmitting stored mobile wallet application information associated with the user to the mobile terminal; receiving mobile terminal information and SE information; and transmitting a stored application associated with the mobile wallet application information to the mobile terminal.
- [13] Exemplary embodiments of the present invention provide a mobile terminal to secure

information over-the-air (OTA) in a non-UICC type SE including an OTA proxy configured to connect to a TSM, and to receive a securing command from the TSM; and a non-UICC type SE.

- [14] It is to be understood that both foregoing general descriptions and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed. Other features and aspects will be apparent from the following detailed description, the drawings, and the claims.

Brief Description of Drawings

- [15] The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention, and together with the description serve to explain the principles of the invention.
- [16] FIG. 1 is a system diagram of a trusted service manager (TSM) ecosystem according to an exemplary embodiment of the present invention.
- [17] FIG. 2 is a system diagram illustrating a method for deleting sensitive credit card credentials and related mobile wallet information from the secure element (SE) and the mobile wallet application according to an exemplary embodiment of the present invention.
- [18] FIG. 3 is a system diagram illustrating a method for synchronizing mobile wallet application to authenticate the mobile terminal and SE accessing the wallet management system according to an exemplary embodiment of the present invention.
- [19] FIG. 4 is a system diagram illustrating a method for reconstructing the financial information credentials and related mobile wallet application through a push method according to an exemplary embodiment of the present invention.
- [20] FIG. 5 is a system diagram illustrating a method for reconstructing financial information credentials and related mobile wallet application through a pull method according to an exemplary embodiment of the present invention.

Mode for the Invention

- [21] The invention is described more fully hereinafter with references to the accompanying drawings, in which exemplary embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these exemplary embodiments are provided so that this disclosure is thorough, and will fully convey the scope of the invention to those skilled in the art. It will be understood that for the purposes of this disclosure, "at least one of each" will be interpreted to mean any combination the enumerated elements following the respective language, including combination of multiples of the enumerated elements. For example, "at least one of X, Y,

and Z” will be construed to mean X only, Y only, Z only, or any combination of two or more items X, Y, and Z (e.g. XYZ, XZ, and YZ). Throughout the drawings and the detailed description, unless otherwise described, the same drawing reference numerals are understood to refer to the same elements, features, and structures. The relative size and depiction of these elements may be exaggerated for clarity, illustration, and convenience.

[22] FIG. 1 is a system diagram of a trusted service manager (TSM) ecosystem according to an exemplary embodiment of the present invention.

[23] As shown in FIG. 1, an example system employing TSM technology with over-the-air (OTA) proxy provisioning includes a TSM 10; mobile terminal 11; network 15; third party messaging platform 16; financial institution 18; mobile network operator (MNO) 19; handset manufacturer 20; and a card manufacturer 21. Before TSM 10 may be fully utilized by the user and its participants, service providers (SP) such as identified in 18 - 21 may go through a pre-registration process. In an example, the network 15 may refer to a cellular network, which may include one or more base stations to enable mobile terminal 11 to communicate with other mobile terminals or third party entities. In addition, network 15 may also include any other type of suitable communication network, such as the Internet, traditional wired telephone lines, and other suitable network technologies.

[24] The handset manufacturers 20 may include embedded secure element (SE) producers, and card manufacturers 21 may include producers of micro secure digital (SD) SE (i.e. non-Universal Integrated Circuit Card (UICC) SEs). As different SE manufacturer may provide for OTA keys that are different from the OTA keys provided for traditional UICC SE devices, handset manufacturers 20 and card manufacturers 21 may provide their OTA keys to TSM 10 in the pre-registration process mentioned above for future processing. Alternatively, the handset manufacturers 20 and card manufacturers 21 may provide their respective OTA keys upon request without going through the pre-registration process. A more detailed explanation of the pre-registration process is provided in the co-pending application 61/428,853.

[25] In an example, OTA proxy may be initialized or configured to be connected with TSM 10 during usage of a mobile wallet application to conserve technical resources. As such, OTA proxy will be in a sleep mode as a default until it is awoken for its utility. To provide for an awakening mechanism, a third party messaging platform 16 (e.g. Cloud to Device Messaging (C2DM)) may be utilized to wake the OTA proxy, which in turn will connect with the TSM 10 for usage. If the TSM 10 sends a message to a third party messaging platform 16 with the wake-up command and identifying information, the third party messaging platform 16 in turn sends a message to the identified mobile terminal 11 to wake up OTA proxy residing within the mobile

terminal 11. Once awake, OTA proxy will connect to the TSM 10 for provisioning or other utility. Alternatively, if desired, OTA proxy may be connected at higher frequencies or continuously to avoid the wake-up process described above.

- [26] If mobile terminal 11 is equipped with a Near Field Communication (NFC)-enabled chip and provisioned with contactless card applets that may use NFC technology, the owner of the mobile terminal 11 may make a purchase at the NFC enabled Point-of-Sale (POS) merchant by waving the mobile terminal 11 at the corresponding POS device. Subsequently, once a purchase is made with the mobile terminal 11, the acquirer network 23 and payment processor 22 may work together to ensure the payment gets updated at the financial institution 18. This end user application, however, does not involve the described TSM ecosystem and is illustrated to provide a description of a complete ecosystem.
- [27] A method for deleting of sensitive information, such as credit card credentials, from the SE of the mobile terminal is described below in reference to FIG. 2. While only the method for deletion is described in this exemplary figure, it will be understood other methods for securing sensitive information may be used, such as locking access to information stored in the SE.
- [28] FIG. 2 is a system diagram illustrating a method for deleting sensitive credit card credentials from the SE. For purposes of the present disclosure, although not illustrated in FIGS. 2 - 5, it will be understood that any communication that is conducted between the external parties or service providers (18-21), TSM 10, and the mobile terminal 11 is provided through Network 15 as shown in FIG. 1 or other suitable methods. Further, it will be understood that the sensitive information is not limited to credit card information, and the reference to credit card information is used merely as an example for the purposes of this disclosure.
- [29] As shown in FIG. 2, in step 201, Service Provider (SP), such as Financial Institution 18, makes a request with the identifying information, such as a Mobile Subscriber Integrated Services Digital Network (MSISDN) to delete its credentials (e.g. credit card number, expiration date, security code, personal identification number (PIN)) from the stolen/lost mobile terminal 11. In an example, such a request may be initiated by the owner of the mobile terminal 11 or the individual SP. The request may be specific to the credit card information belonging to a specific SP or it may be to delete the all of credit card information residing in the SE, if not all of the sensitive information stored within the SE. While the request may typically be limited to only the credit card information belonging to the requesting SP, if an agreement is met by various financial institutions, credit card information of other agreeing SPs may be also deleted.
- [30] Likewise in step 201, the request sent by the SP may be to lock the entire SE containing credit card credentials, or to lock just the respective secure domain within

the SE, which stores the respective credit card information. The request for locking or deleting specific security domain or SE may be specified by the SPs or may be catered to meet other business rules/requirements. In addition, while not illustrated in the provided figure, the request to secure the information stored in the SE may be initiated by the mobile terminal 11 owner contacting the TSM 10 directly. Also, the request in step 201 may be initiated by SP by its own volition or in response to a request by the owner of the mobile terminal 11.

- [31] In step 202, the TSM 10 receives the request from SP and updates the respective mobile terminal account to “delete” status within its database. In addition, TSM 10 conducts an internal query to verify whether the mobile terminal 11 in question has a mobile wallet application 31 installed, such as a SK C&C mobile wallet application 31. In an example, if the TSM 10 determines that a SK C&C mobile wallet application 31 is installed in the respective lost/stolen mobile terminal 11, TSM 10 modifies the request to delete related contactless applets, Wallet Management Application (WMA) 21 credit card credentials residing within the SE (wallet management applets), and the widgets residing within the SK C&C mobile wallet application 31.
- [32] In addition, TSM 10 makes a determination on the type of SE equipped on the lost/stolen mobile terminal 11. As Micro SD's and Embedded SEs (i.e. non-UICC type SEs) cannot support conventional Subscriber Identity Module Application Toolkit (SAT) / Universal Subscriber Identity Module Application Toolkit (USAT) / Card Application Toolkit (CAT) framework, the deletion command composed by TSM 10 may go through OTA proxy in order to make any deletion of the information stored in the non-UICC type SEs, such as microSDs or embedded SEs. However, OTA proxy may also support SEs supported by traditional SAT/USAT/CAT framework as well, such as UICC, Services Identity Module (SIM), or Universal Subscriber Identity Module (USIM) (herein referred collectively as UICC). A more detailed explanation on the OTA proxy may be found in the co-pending application 61/428,851.
- [33] Once TSM 10 completes modifying the user account status, a push request is made to mobile push server, such as a Cloud to Device Messaging (C2DM) platform, in step 203.
- [34] In step 204, the mobile push server pushes the message to wake up the OTA proxy residing in the lost/stolen mobile terminal 11.
- [35] In step 205, the OTA proxy retrieves mobile terminal 11 and associated SE specific information such as MSISDN and Card Image Number (CIN) and sends them to TSM 10. In an example, SE information may also include Card Reference Number (CRN), Card Production Life Cycle (CPLC), and Card Serial Number (CSN).
- [36] Further, although not illustrated, once TSM 10 receives mobile equipment and SE information, TSM 10 checks the status of SE. As processing of stored SE may be based

on its status, analysis of SE status and corresponding processes may be conducted prior to accessing the information stored in the SE. More specifically, based on the SE status, some preparation steps may be executed to secure the SE for processing commands received through the OTA proxy. In an example, SE equipped in the mobile terminal 11 may have any of the 3 statuses: operating system (OS) native, initialized, and secured. If the status of the SE is determined to be “secured” no further preparation steps may be executed. The “secured” state for the SE may refer to an intended operating card life cycle state in post issuance. On the other hand, if the status of the SE is determined to be “initialized” then TSM 10 may provide a final issuer master key to secure the SE. The “initialized” state for the SE may refer to an administrative card production state. Lastly, if the status of the SE is determined to be “OS native”, then pre-personalization process may be conducted, which may include providing an initial issuer master key and a final issuer master key to the SE. The “OS native” state for the SE may refer to a status that SE is not initialized by manufacturer’s initialization method.

- [37] After status of the SE has been determined, an analysis of SE type may be performed to determine the type of protocol that should run within OTA proxy in order to provision into the identified SE. If the SE is a UICC type or an embedded type, SE may be accessed to modify the information stored in the SE. Alternatively, if the SE is a Micro SD type, additional process specific protocol may be executed to access or to modify the information stored in the SE. Since a person ordinarily skilled in the art understands what type of protocols may be used to access the Micro SD type, discussion thereof is omitted herein.
- [38] In step 206, TSM 10 processes the provided information along with the “delete” command and converts them into Application Protocol Data Unit (APDU) commands and sends the converted APDU commands to the OTA proxy.
- [39] In step 207, OTA proxy relays the received APDU commands to the SE where credit card credentials may reside. Credit card credentials may reside as contactless card applets as well as within a wallet management applet (WMA) 21. Please refer to the co-related application number 61/428,846 for further details on how a corresponding WMA 21 is created.
- [40] Once the “delete” command has been processed successfully, results are sent to the OTA proxy in step 208.
- [41] In step 209, OTA proxy relays the result back to the TSM 10. TSM 10 in turn sends a notification to the SP of the outcome of its request in step 210.
- [42] The “delete” functionality disclosed in FIG. 2 may be provided if the mobile terminal 11 is powered on and has reception to a network.
- [43] In FIG. 3, a system diagram is provided for synchronizing the mobile wallet ap-

plication 31 residing within the mobile terminal 11.

[44] In step 301, multiple external parties or SPs may request changes to be made to user's mobile wallet application 31 configuration using the TSM/ Wallet Management System (WMS), which may store the master configuration of the user's mobile wallet application 31. For the purposes of this disclosure, the external parties or SPs may include, without limitation, Financial Institutions 18, Mobile Network Operator (MNO) 19, Handset Manufacturer 20, and Card manufacturer 21 (collectively referred to as "service providers" or "SPs"). As the mobile wallet application 31 may not always be on, the TSM/WMS may serve as a central repository to allow various external parties to make change requests without regard to user's login status to the mobile wallet application 31. For example, the respective external parties or SPs may request additional contactless cards to be provisioned to the user's mobile wallet application 31 on their own time without regard to the user's status.

[45] Similarly, TSM 10 itself may automatically recognize that the expiration date of a contactless card applet stored in the SE is approaching based on its own internal records and prompt the user to renew the contactless card applet information. In an example, the user of the mobile terminal 11 may be prompted by the mobile wallet application 31 or other suitable methods, such as emails, texts, and voicemails. User may be prompted by the TSM 10 by other methods as well, such as texts, emails, voicemails or other suitable methods of providing notification. In response to the prompt, the user of the mobile terminal 11 may re-provision the respective contactless card applet through the TSM 10 system or by contacting the SP responsible for the soon to be expired contactless card applet.

[46] Subsequently, in step 302, when the user logs into the mobile wallet application 31 on the mobile terminal 11, the OTA proxy residing within the mobile wallet application 31 will retrieve specific mobile terminal 11 information and SE specific information (e.g. MSISDN, International Mobile Equipment Identity (IMEI) / Mobile Equipment Identifier (MEID), CIN/ Integrated Circuit Card Identification (ICCID)) and send them to TSM 10 for analysis.

[47] In step 303, TSM 10 upon receipt of the provided information, conducts an internal verification of the provided information by OTA proxy with the stored information.

[48] If it is found that the provided handset information or the SE information conflicts with the registered information, the TSM 10 logs the event and may order the mobile wallet application 31 to lock or delete sensitive information until further verification or clarification can be provided in step 304. Sensitive information may include account specific information related to financial institution 18 that may be stored in the SE, such as credit card numbers, expiration date, personal identification number, and other related information. Further, sensitive information may also include user security in-

formation or other private information stored in the SE.

- [49] In an example, a thief may steal a removable SE, such as a micro SD, from a mobile terminal 11 and use it on a different mobile terminal before the user even realizes the SE is missing from his or her mobile terminal 11. By cross referencing the registered SE with the registered mobile terminal identification, TSM 10 will recognize whether the registered SE is being equipped on different non-registered mobile terminal 11. Further, it should be noted that TSM 10 may handle recognition of inconsistent devices in a different manner than described in step 304. TSM 10 may handle such an event according to the business rules provided by the parties involved, such as opting to prompt the user for a password, security key, or other verification methods.
- [50] Additional or different directions may be provided by the consumers or SPs in handling such event according to their business rules.
- [51] This synchronization check may also be conducted when a request is made to provision another contactless card applet 23 or whenever OTA proxy is requested to connect with the TSM 10 or equivalent system.
- [52] FIG. 4 illustrates an exemplary system diagram of a push system for reconstructing mobile wallet application 31. Once the user has found or replaced the mobile terminal, which may no longer contain all of the previous the user's financial credentials, the user of the device may contact one of the SPs or TSM 10 to reconstruct its mobile wallet application 31 and all of the previously stored contents therein. For the purposes of the present disclosure, mobile wallet application 31 may include the widgets residing within the mobile wallet application 31, contactless card Applet 23 and associated WMA 21 stored in the SE, and an optional OTA proxy. However, a mobile wallet application 31 may include less than all of the elements described herein or more than the elements described herein.
- [53] In step 401, the user of the mobile terminal 11 contacts SP notifying procurement of a new mobile terminal 11. SP may conduct its own authentication to verify the correct user of the mobile terminal 11. Similarly, the user may also notify MNO 19 or TSM 10 directly as well.
- [54] Once SP has authenticated the user, SP sends a request to TSM 10 to re-provision the user's new mobile terminal 11 with the SP's contactless application and related credentials in step 402.
- [55] In step 403, TSM 10 performs an internal check to verify whether the user has any other SP accounts that it had provisioned prior to losing his or her phone. If there are other SP accounts held by the user, a request is made to the respective SPs for its provisioning information.
- [56] Once SPs receive requests for provisioning information, internal authentication and validation check may be conducted and the necessary information sent to TSM 10 for

processing in step 404.

- [57] In step 405, another internal check is conducted to verify what mobile wallet application 31 the user previously had in his or her mobile terminal 11. The mobile wallet application 31 may include various types, such as a SK C&C mobile wallet application 31 or other mobile wallet applications offered by different manufacturers.
- [58] In an example, if it is found that the mobile wallet application 31 was previously installed, then the system will retrieve the same version and user preference settings associated with the mobile wallet application 31 to transmit to the user in step 406. The respective mobile wallet application 31 along with its configured user preferences may be sent to the user mobile terminal 11 through a mobile push server prior to moving to step 407. For the purposes of this disclosure, it is assumed the mobile wallet application 31 includes a corresponding OTA proxy, which may be installed by the mobile terminal 11 upon receipt of the application or by a separate process.
- [59] In step 407, TSM 10 sends a push message to wake up OTA proxy to a mobile push server, such as a C2DM system. In an example, the mobile wallet application 31 may be sent prior to OTA proxy, at the same time as the mobile wallet application 31, or before the mobile wallet application 31.
- [60] Subsequently, the mobile push server relays the received wake up command to OTA Proxy in step 408.
- [61] In step 409, the OTA proxy retrieves mobile terminal 11 and SE specific information such as MSISDN and CIN and sends it to TSM 10.
- [62] Once TSM 10 receives the information sent by OTA Proxy, TSM 10 processes the information along with the provisioning commands and converts them into APDU commands to send over to OTA proxy in step 410. In an example, the provisioning commands may include specific instructions, such as install or delete specific information or application, and account specific information for a contactless card applet, which may be provided by the Financial Institution 18. Also, when account specific information is received for the contactless card applet or other sensitive information, such information may be duplicated to be provisioned into the WMA 21. In addition, a version of the associated widget for the mobile wallet application 31 of the mobile terminal 11 is also obtained by the TSM 10 to be provisioned directly into the wallet application 31.
- [63] Next, in step 411, OTA proxy relays the received APDU commands to the SE where credit card credentials, contactless applets, may be provisioned. If the user was a previous user of a mobile wallet application 31, APDU commands will be relayed to provision account information corresponding to the contactless applets to be installed within the WMA 21, which is also located within the SE. In addition, corresponding widget application will be installed in the mobile wallet application 31 to provide a

graphic display of the installed account.

[64] Once the provisioning command has been successfully processed, results are sent back to the OTA proxy in step 412.

[65] Subsequently, OTA Proxy relays the results back to the TSM 10 in step 413 and the TSM 10 updates its system with the results of the request.

[66] Notification of the outcome of the SP provisioning request is sent to the respective SP(s) in step 414.

[67] Similarly to FIG. 4, the user's mobile wallet application 31 may be reconstructed through a pull mechanism, which may be initiated by the mobile terminal 11 owner as illustrated in FIG. 5.

[68] In step 501, the owner of the mobile terminal 11 attempts to reinstall the mobile wallet application 31 from the mobile terminal 11 and a request is made from the new or replaced mobile terminal 11. A command request is sent along with mobile identification information to TSM 10.

[69] TSM 10 receives the request with its related identification information, and in step 502, an authentication process takes place to verify the user. The requesting user may be verified through a password, security question, social security number, or through other suitable verification methods. Once the user has been correctly identified, a check is conducted for an existing account. If it is found that a mobile wallet application 31 was previously installed, then the system will retrieve the same version and user preference settings related to the mobile wallet application 31 and send to the user in step 503 for downloading. The respective mobile wallet application 31 along with its configured user preferences may be sent to the user mobile terminal 11 through a mobile push server.

[70] In an example, if it is determined that the requesting user did not have a mobile wallet application 31 previously, a new account is created in the TSM 10 and a mobile wallet application 31 may be sent to the mobile terminal 11 through a mobile push server. For the purposes of this disclosure, it is assumed the mobile wallet application 31 includes a corresponding OTA proxy, which may be installed by the mobile terminal 11 upon receipt of the application or by a separate process.

[71] Next, in step 504, TSM 10 checks the requesting user account for related SP account information. If one or more SP accounts are associated with the requesting user's account, notification may be sent to each SP, requesting provisioning information to be sent to the requesting user. While steps 503 and 504 were configured as separate steps, steps 503 and 504 may be conducted in conjunction or in a reverse order as well. For example, the present disclosure provides for a mobile wallet application 31 and widgets related to the SP separately. However, it may also be possible to gather all of the necessary widgets and the mobile wallet application 31 from the SP, so that the TSM

10 can relay both the widgets and the mobile wallet application 31 simultaneously to the user. Alternatively, if TSM 10 is allowed to store account specific information, the mobile wallet application 31 and the widgets may be provided by the TSM 10 without making additional requests to the SPs.

[72] Once SPs receive requests for provisioning information, internal authentication and validation check may be conducted and the necessary information sent to TSM 10 for processing in step 505.

[73] In step 506, TSM 10 sends a push message to wake up OTA proxy to the mobile push server, such as a C2DM system. While it is illustrated that mobile wallet application 31 is sent prior to OTA proxy, it should be noted that OTA proxy may be sent at the same time as the mobile wallet application 31, or before the mobile wallet application 31 as well.

[74] Subsequently, the mobile push server relays the received wake up command to OTA Proxy in step 507.

[75] In step 508, the OTA proxy gathers mobile terminal 11 specific information such as MSISDN and CIN along with the provisioning commands and sends it to TSM 10. In an example, the provisioning commands may include specific instructions, such as install or delete specific information or application, and account specific information for a contactless card applet, which may be provided by the Financial Institution 18. Other sensitive information such as a key to the SE may be provided either by the other SPs or the TSM 10. Sensitive information may be provided by the SPs in real-time using the TSM 10 as an intermediary or in advance for storage in the TSM 10.

[76] Once TSM 10 receives the information sent by OTA Proxy, TSM 10 processes the information along with the provisioning commands and converts them into APDU commands and sends them to OTA proxy in step 509. Also, if provisioning commands including account specific information of the contactless card applet is received, such information may be duplicated to be provisioned into the WMA 21. In addition, a version of the associated widget for the wallet application 31 is also obtained by the TSM 10 to be provisioned directly into the mobile wallet application 31.

[77] Next, in step 510, OTA proxy relays the received APDU commands to the SE where credit card credentials, contactless applets, may be provisioned. If the user was a previous mobile wallet application 31 user, APDU commands may be relayed to provision account information corresponding to the contactless applets to be installed within the WMA 21, which is also located within the SE. In addition, corresponding widget application may be installed in the mobile wallet application 31 to provide a graphic display of the installed account.

[78] Once the provisioning command has been successfully processed, results are sent back to the OTA proxy in step 511.

- [79] Subsequently, OTA Proxy relays the result back to the TSM 10 in step 512 and the TSM 10 will update its system with the result of the request.
- [80] Notification of the outcome of the SP provisioning request will be sent to the respective SP(s) in step 513.
- [81] It will be apparent to those skilled in the art that various modifications and variation can be made in the present invention without departing from the spirit or scope of the invention. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

Claims

- [Claim 1] A method for securing information in a non-Universal Integrated Circuit Card (UICC) type secure element (SE) of a mobile terminal, comprising:
receiving a request to initialize an over-the-air (OTA) proxy of a mobile terminal;
initializing the OTA proxy;
receiving a request to secure information stored in the SE; and
securing, using the OTA proxy, the information stored in the SE, wherein the SE is a non-UICC type SE.
- [Claim 2] The method of claim 1, further comprising:
requesting installation of the OTA proxy;
receiving OTA proxy installation information; and
installing the OTA proxy in the mobile terminal.
- [Claim 3] The method of claim 2, wherein OTA proxy installation information is received from a Trusted Service Manager (TSM).
- [Claim 4] The method of claim 3, wherein initializing the OTA proxy comprises:
waking the OTA proxy; and
transmitting mobile terminal information and SE information to the TSM,
wherein the SE information comprises an SE status and an SE type.
- [Claim 5] The method of claim 1, wherein the request to secure information comprises an Application Protocol Data Unit (APDU) command.
- [Claim 6] The method of claim 5, wherein securing the requested information in the non-UICC type SE comprises executing the APDU command for securing the requested information, wherein the non-UICC type SE comprises a Micro Secure Digital (SD), an Embedded SE, or a SE that does not support either a Short Message Service Point to Point (SMS-PP) protocol or a Bearer Independent Protocol (BIP).
- [Claim 7] The method of claim 1, wherein securing the requested information in the SE comprises deleting information stored in the non-UICC type SE.
- [Claim 8] The method of claim 1, wherein securing the requested information in the SE comprises locking access to information stored in the non-UICC type SE.
- [Claim 9] The method of claim 1, wherein the request to initialize the OTA proxy is received from a push server.
- [Claim 10] The method of claim 1, further comprising preparing the SE for

securing information before securing the requested information,
wherein preparing the SE comprises:
retrieving mobile terminal information and SE information, wherein the
SE information comprises an SE status and an SE type;
receiving a key based on the SE status; and
using the key to access the SE.

- [Claim 11] The method of claim 10, wherein the mobile terminal information comprises at least one of International Mobile Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), and Mobile Subscriber Integrated Services Digital Network Number (MSISDN).
- [Claim 12] The method of claim 10, wherein the key comprises at least one of an initial issuer master key and a final issuer master key.
- [Claim 13] The method of claim 12, wherein securing the information stored in the SE comprises providing at least one of the initial issuer master key and the final issuer master key to the SE in response to a determination that the SE status is Operating System (OS) native.
- [Claim 14] The method of claim 12, wherein securing the information stored in the SE comprises providing the final issuer master key to the SE in response to a determination that SE status is initialized.
- [Claim 15] The method of claim 10, wherein using the key to access the SE further comprises processing a protocol for enabling provisioning of the SE, the SE type being a Micro Secure Digital (SD) type.
- [Claim 16] A method for authenticating a mobile terminal, comprising:
receiving mobile terminal information and secure element (SE) information from the mobile terminal;
comparing the received information with stored mobile terminal information and SE information; and
transmitting a command based on the comparison result.
- [Claim 17] The method of claim 16, wherein the mobile terminal information comprises at least one of International Mobile Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), and Mobile Subscriber Integrated Services Digital Network Number (MSISDN).
- [Claim 18] The method of claim 16, wherein the SE information comprises at least one of Card Image Number (CIN), Card Reference Number (CRN), Card Production Life Cycle (CPLC), and Card Serial Number (CSN).
- [Claim 19] The method of claim 16, wherein transmitting a command based on the comparison result comprises transmitting a command to delete information stored in the SE of the mobile terminal, in response to the

- received information being different from the stored information.
- [Claim 20] The method of claim 19, wherein the SE is a non-Universal Integrated Circuit Card (UICC) type SE.
- [Claim 21] The method of claim 16, wherein transmitting a command based on the comparison result comprises transmitting a command to lock access to the information stored in the SE of the mobile terminal, in response to the received information being different from the stored information.
- [Claim 22] The method of claim 21, wherein the SE is non-UICC type SE.
- [Claim 23] A method for reconstructing a mobile wallet application of a mobile terminal, comprising:
receiving a request to reconstruct the mobile wallet application of a user;
transmitting stored mobile wallet application information associated with the user to the mobile terminal;
receiving mobile terminal information and secure element (SE) information; and
transmitting a stored application associated with the mobile wallet application information to the mobile terminal.
- [Claim 24] The method of claim 23, wherein transmitting stored mobile wallet application information associated with the user to the mobile terminal comprises transmitting an over-the-air (OTA) proxy application associated with the user.
- [Claim 25] The method of claim 23, wherein transmitting stored mobile wallet application information associated with the user to the mobile terminal comprises transmitting an OTA proxy application associated with the mobile wallet application information.
- [Claim 26] The method of claim 23, wherein receiving a request to reconstruct the mobile wallet application comprises receiving identifying information associated with the user.
- [Claim 27] The method of claim 23, wherein the stored application information associated with the mobile wallet application comprises at least one of a contactless card applet, a wallet management applet, and a widget application for interfacing the user.
- [Claim 28] A mobile terminal to secure information over-the-air (OTA) in a non-Universal Integrated Circuit Card (UICC) type secure element (SE), comprising:
an OTA proxy configured to connect to a Trusted Service Manager (TSM), and to receive a securing command from the TSM; and

a non-UICC type SE.

[Claim 29]

The mobile terminal of claim 28, wherein the securing command is a command to delete information stored in the non-UICC type SE or to lock access to information stored in the non-UICC type SE.

[Claim 30]

The mobile terminal of claim 28, wherein the OTA proxy is configured to transmit mobile terminal information and SE information to the TSM, wherein the SE information comprises an SE status and an SE type.

[Claim 31]

The mobile terminal of claim 30, wherein the OTA proxy is further configured to receive a key from the TSM to access the SE based on the SE information sent to the TSM, wherein the key comprises at least one of an initial issuer master key and a final issuer master key.

[Claim 32]

The mobile terminal of claim 30, wherein the OTA proxy is further configured to receive a protocol to prepare the SE to be provisioned, the SE type being a Micro Secure Digital (SD) type.

[Claim 33]

The mobile terminal of claim 28, wherein the non-UICC type SE comprises:

a contactless card applet; and

a wallet management applet corresponding to the contactless card applet, wherein the wallet management applet comprises at least one of an account number associated with the contactless card applet, an expiration date, and a security code.