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. The~~

~~[Claim 20] method of claim 19, wherein the SE is a non-Universal Integrated Circuit Card (UTCC) 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 16~~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,

wherein the mobile terminal is used in a method for securing the information, the method comprising :

receiving a request to initialize the OTA proxy of the mobile terminal;

initializing the OTA proxy;

receiving a request to secure the 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 17~~29~~] The mobile terminal of claim 16~~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 18~~30~~] The mobile terminal of claim 16~~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 19~~31~~] The mobile terminal of claim 18~~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 20~~32~~] The mobile terminal of claim 18~~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 21~~33~~] The mobile terminal of claim 16~~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.