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

[7A] The present invention provides a method for securing information stored 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.

[7B] The present invention also provides 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 comments 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 an over-the-air (OTA) proxy of the 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.

[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